Modeling and Simulation in Support of

Network Centric Warfare Analysis

Chris Alspaugh, Dr. Nikhil Davé, Tom Hepner, Andy Leidy, Dr. Mark Stell,
Dr. Cam Tran, Heather Woods, Wonita Youm, Dr. Albert Legaspi
SPAWAR Systems Center San Diego
Code 2822 Network Centric Warfare Analysis Branch
53560 Hull Street
San Diego, CA 92152-5001

{chris.alspaugh, nikhil.dave, tom.hepner, andy.leidy, mark.stell, cam.tran, heather.woods,
wonita.youm, albert.legaspi}@navy.mil

Jim Weatherly
Navy Modeling and Simulation Management Office (NAVMSMO)
OPNAV N61F21
2000 Navy Pentagon PT 5453
Washington, D.C. 20350-2000

james.weatherly@navy.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Modeling and Simulation in Support of Network Centric Warfare Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **SPAWAR Systems Center San Diego,Code 2822 Network Centric Warfare Analysis Branch,53560 Hull Street,San Diego,CA,92152-5001**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**70**	

Modeling and Simulation in Support of Network Warfare Analysis

Chris Alspaugh, Dr. Nikhil Davé, Tom Hepner, Andy Leidy, Dr. Mark Stell, Dr. Cam Tran, Heather Woods, Wonita Youm, Dr. Albert Legaspi
SPAWAR Systems Center San Diego
Code 2822 Network Centric Warfare Analysis Branch
53560 Hull Street
San Diego, CA 92152-5001
{chris.alspaugh, nikhil.dave, tom.hepner, andy.leidy, mark.stell, cam.tran, heather.woods, wonita.youm, albert.legaspi}@navy.mil

Jim Weatherly
Navy Modeling and Simulation Management Office (NAVMSMO)
OPNAV N61F21
2000 Navy Pentagon PT 5453
Washington, D.C. 20350-2000
james.weatherly@navy.mil

Abstract

The Space and Naval Warfare Systems Center San Diego (SSC San Diego) Code 2822, Network Centric Warfare Analysis Branch, has been developing and integrating models of Navy communications systems. These models are used for assessing communications performance in networked operations and the accompanying impact of communications on C4ISR operations. This paper provides an overview and highlights some of our recently completed tasks and ongoing efforts.

1.0 Introduction

Making use of the full spectrum of modeling and simulation environments is one of the key activities of the SSC San Diego Network Centric Warfare Analysis Branch. Fundamental to our branch operations is the development of standard, reusable, interoperable models to reduce cost and enhance model assessment time. We work with all facets of the M&S community, which includes Joint Services, government agencies, deployed operational commands, academia and industry in order to support the Navy, Joint and Coalition forces with the best possible analysis capability.

This paper highlights some of our recently completed tasks and ongoing efforts. Section 2 introduces our modeling and development efforts as the Navy lead for the Joint program *Net*work *War*fare *S*imulation (NETWARS). In this capacity, our branch has been developing communications models of Navy systems for use within the NETWARS program. We have initiated efforts to integrate and federate communications

infrastructures developed in NETWARS and other simulation systems to leverage the strengths of each simulation system and support analysis of Network Centric concepts in operational scenarios. The integration of Navy Simulation System (NSS) and NETWARS is an illustrated example.

Section 3 highlights our work in model development by way of our Navy Link-16 M&S efforts. In February 2004, the NETWARS Program Management Office decided to adopt our Link-16 model as the standard for Link-16 modeling for Joint Services. Furthermore, our modeling and simulation (M&S) efforts also support Knowledge Superiority and Assurance (KSA) Future Naval Capability (FNC) projects sponsored by Office of Naval Research (ONR). Section 4 depicts two selected studies: the first illustrates the use of M&S to examine ways of constructing a single worldwide 300-ship Navy network that supports ship-to-shore communications; and the second effort involves simulation-assisted routing design for integration of Joint Tactical Radio System (JTRS)-like radios, such as the VRC-99 A/B, into Naval data networks.

SSC San Diego Network Centric Warfare Analysis Branch also initiates and engages in efforts to support and complement a full spectrum of M&S environments. Section 5 provides two examples. One is the DARPA-funded Non-Intrusive Knowledge Suite for monitoring network and application performance. The other is the noteworthy ongoing activity in lab and field experimentation in support of FORCEnet and the Joint Rapid Architecture Experiment (JRAE). A concluding remark on our M&S missions and capabiliies is provided in Section 6.

2.0 Navy Network Warfare Simulation (NETWARS)

The *Net*work *War*fare *S*imulation (NETWARS) program is managed jointly by the Command, Control, Communications, and Computer (C4) Systems Directorate of the Joint Staff (J-6) and the Defense Information Systems Agency (DISA). NETWARS, the network modeling and simulation (M&S) tool, is designed to assess military communications networks. Its intended use is to conduct simulations at the joint task force level, involving thousands of networked participants with tens of thousands of messages, down to the tactical unit level [1].

The Space and Naval Warfare Systems Center at San Diego (SSC San Diego), the US Navy C4ISR laboratory, is involved in developing communications models of Navy systems for use within the NETWARS program. We are supporting NETWARS by developing high-fidelity models of its communications systems [2, 3]. Furthermore, to assess military communications networks and the impact of communications on C4ISR operations, we realize that by federating NETWARS with other M&S tools we can leverage each tool's strengths. Our effort [4] to integrate the force-on-force M&S tool Naval Simulation System (NSS) [5] with NETWARS is under development.

2.1 NETWARS Architecture

NETWARS is a discrete event simulator developed using the Optimized Network Engineering Tool (OPNET) Development Kit (ODK). It has been designed to analyze military communications networks through the use of reusable communications device models (CDM), military doctrine, and network traffic information in the Joint arena. NETWARS consists of four functional elements, which are: 1) Database libraries; 2) Scenario Builder; 3) Simulation Domain; and 4) Analytical Tools. Figure 1 illustrates the relationship among these functional elements.

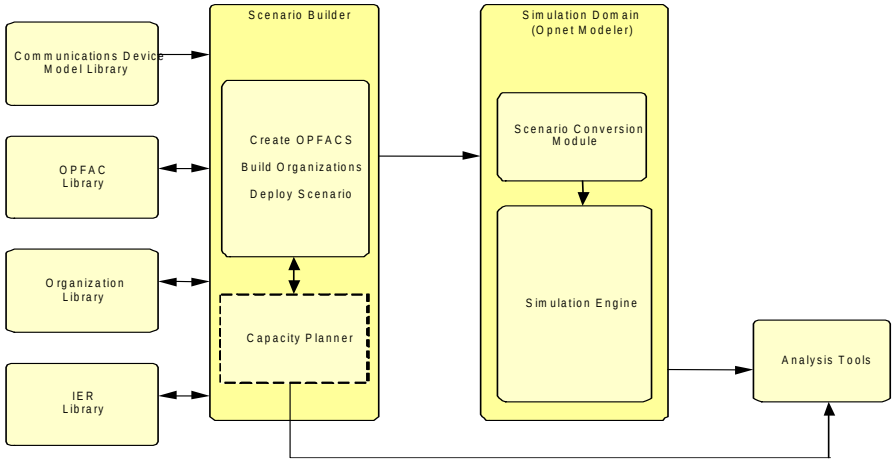


Figure 1. NETWARS System Architecture.

2.1.1 Database Libraries

NETWARS makes use of four primary databases. They are the: 1) Communications Device Model Library; 2) Operations Facilities (OPFAC) Library; 3) Organization Library; and 4) Information Exchange Requirements (IER) Library. The simulator uses these libraries to obtain detailed information about the communications systems used during the analysis. The CDM library contains the fundamental building blocks used in NETWARS. This library contains the models that have been developed by the services to represent the protocols and functionality that is found in real physical devices. Examples of Navy CDMs include radios, patch panels, multiplexers and tactical communications data links. The OPFAC library is used to represent logical collections of CDMs, such as a tank or a Naval Operations Center (NOC). The Organization library is built from one or more OPFACS that are connected with various communications links, which include point-to-point, wireless, and broadcast links. IERs are used to specify the message traffic that is to traverse the network. IERs are used to provide the simulation with details about the traffic, such as the type of traffic (voice, video, or data), the source and destination of the message, its size, and the frequency with which the message is sent.

2.1.2 Scenario Builder

The Scenario builder is used to define how the OPFACS, Organizations, links, and IERs are to be used during the simulation. OPFACS and Organizations can be developed, and links can be assigned. Mobility can be given to Organizations to represent the realtime movement of units throughout the course of the simulation. IERS are associated with devices, and the times in which the IERS are sent are also defined here. Periods of failure and recovery of OPFACS are also specified within the Scenario Builder.

2.1.3 Simulation Domain

The Simulation Domain provides for the conversion of scenario information into a common Scenario Definition File (SDF), that in theory, can be submitted to any simulation engine that supports the SDF format. At this time, the SDF file is fed into the OPNET simulation engine. This is a commercial, off the shelf (COTS) discrete event simulator that is used to assess the traffic flowing across the network.

2.1.4 Analysis Tools

The Analysis Tools provide a way to examine the results of the simulation. They allow the analyst to examine the measures of performance (MOPs) that were collected during the simulation. A sampling of the MOPs that NETWARS monitors during a simulation include link utilization, throughput, message delay, and message completion and failure rate. The program can also collect node-level statistics, or other custom statistics if the user incorporates the collection of these statistics within the appropriate CDMs.

2.1.5 HLA Interface

NETWARS also can make use of a High Level Architecture (HLA) interface to permit communications between the NETWARS simulator and other simulators. A beta version of an HLA module for NETWARS has been under development by DISA and OPNET Technologies, Inc., however it is not part of the official NETWARS release.

As the NETWARS communications simulation environment continues to mature and grow in popularity within the DoD, the US Navy has initiated parallel and follow-up investigations into the integration of NETWARS with other simulators for HLA cosimulations. The integration of the Naval Simulation System (NSS) and NETWARS allows users to leverage NETWARS high-fidelity communications models to enhance advanced capabilities of NSS in Naval operation support (including plan development, evaluation, refinement, and execution) and analysis at the mission, group, and force levels [4]. This integration ultimately allows the user to federate NSS with NETWARS through an HLA Runtime Infrastructure (RTI), therefore promoting software reuse and interoperability between these two modeling and simulation tools. In FY04, we will run POM-06 scenarios provided by OPNAV N81 to support PR-07 analysis.

2.2 An Example

An example of the use of NETWARS as a tool is our modeling of the Network Operations Center (NOC) that is currently being developed at SSC-San Diego. There are four NOCs worldwide, however each NOC has its unique differences. The Pacific Region NOC (PRNOC, in Wahiawa, HI) was considered the most generic of the four and so it was used as the template Organization. This template NOC Organization included three Organizations within it: the Secure Internet Protocol Router Network (SIPRNET) enclave, the Non-secure Internet Protocol Router Network (NIPRNET) enclave, and the Automatic Digital Network System (ADNS) enclave.

Within each of these three enclaves were several OPFACs that represented different network devices such as routers, switches, computers, and mutliplexers. Several of these OPFACs were created using OPNET model device libraries and thus had to be slightly modified to fulfill the requirements delineated in the NETWARS Model Development Guide (MDG) [6].

Figure 2 depicts OPFACs of the NIPRNET and ADNS Organizations. Because NETWARS currently does not support intra-OPFAC traffic, a detailed study requires partitioning NIPRNET into many small OPFACs. This limitation is known and a software change request was submitted for future enhancement.

Building upon and modifying the template NOC Organization enabled the creation of the three other NOCs: the Unified Atlantic Region NOC (UARNOC), the Indian Ocean Region NOC (IORNOC), and the Europe Central Region NOC (ECRNOC).

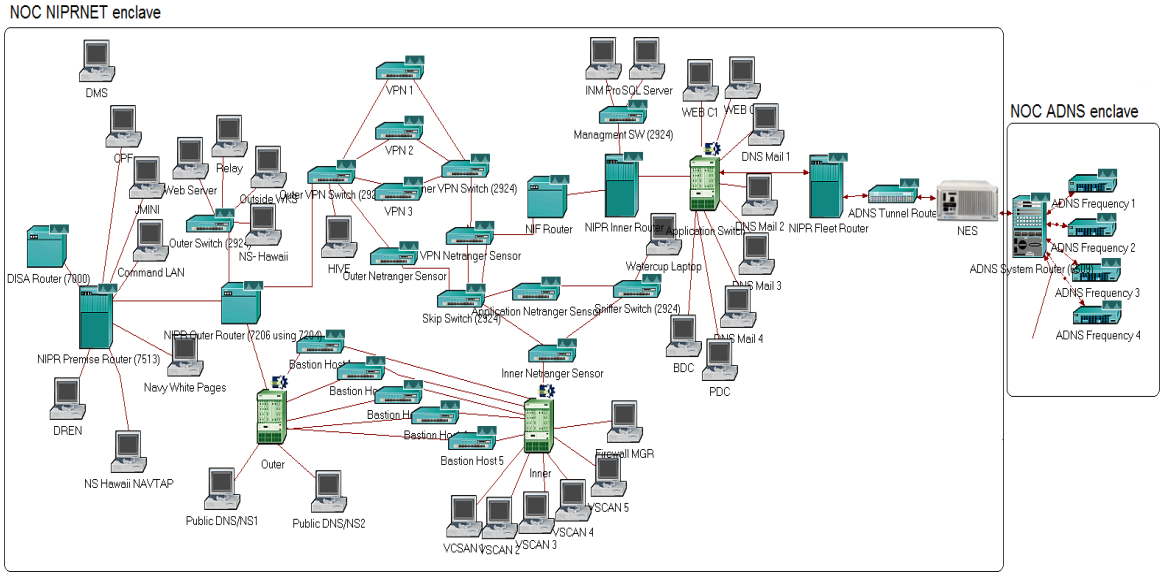


Figure 2. OPFACs of NIPRNET and ADNS Organizations.

3.0 Link-16 Modeling and Simulation (M&S) Efforts

The Network Centric Warfare Analysis branch of the Space and Naval Warfare (SPAWAR) Systems Center San Diego (SSC San Diego) has supported simulation-based assessments for over ten years. During this time, SSC San Diego has accumulated an extensive library of communications models to support analysis that range from capacity planning, to prototype modeling, to military communications planning and doctrine development. Models within the SSC San Diego library are generally interoperable and reusable and may be leveraged to support a wide variety of future studies.

One of the more interesting families of models within the SSC San Diego model library is the Link-16 model suite. These models represent communications characteristics of the Tactical Data Information Link (TADIL) J communication system. They have become increasingly popular throughout the Joint communications M&S community and have supported many simulation studies. The following subsections provide an overview of the Link-16 model architecture and design features.

3.1 Link-16 System Overview

Link-16 is a tactical message exchange system that is being deployed within the military systems of the United States Joint Services, and forces of the North Atlantic Treaty Organization (NATO) [7]. Link-16 represents the latest technology within the TADIL family, which includes Link-11 and Link-4/4A. The general purpose of Link-16 and other TADILs is to exchange real-time tactical data among units within military operations. Tactical data includes information such as target tracking, force orders, and position reporting. While Link-16 is similar in general functionality to other TADILs, it features many significant improvements, such as increased types of data exchange, nodelessness, jam resistance, flexibility, separate transmission and data security, increased numbers of participants, increased data capacity, and secure voice support.

3.2 Link-16 Model Development Evolution

The Link-16 model was originally developed in September 2001 to support a Time Critical Strike (TCS) study that was sponsored by the Assistant Secretary of the Navy for Research, Development, and Acquisition Chief Engineer of the Navy (ASN RDA CHENG). The objective of this study was to assess several TCS scenarios to minimize the time it takes to strike a target under various conditions. Communications performance is essential in the timely detect, decide, engage, and assess life cycle of a time critical targeting scenario. Link-16 was assessed as a possible communications subsystem for TCS information exchange and a model was developed to meet end-to-end assessment requirements.

After the TCS study, the Link-16 model was reused in several simulation-based efforts within SSC San Diego (see, for example, [8]). Throughout these studies, the model was enhanced to meet additional requirements and evolved into a fairly high-fidelity, general-purpose Link-16 communications model. As a result, in 2003, the Link-16 Program

Management Office (PMO), through the Office of Naval Research (ONR), began to use the model for prototyping of potential Link-16 system enhancements. To support these investigations, the Link-16 PMO guided some of later stages of the model enhancements to create a very high fidelity Link-16 simulation capability.

As the lead Navy model developers for NETWARS, SSC San Diego contributed the Link-16 model to the NETWARS model library in January 2003. The NETWARS M&S community has since used it extensively.

In February 2004, the NETWARS PMO decided to adopt the Navy Link-16 model as the standard for Link-16 modeling for all of the Joint Services. SSC San Diego is currently supporting this NETWARS standardization effort, which includes user interface enhancements and additional Joint Range Extension (JRE) support.

3.3 Link-16 Model Suite Overview

There are three device models within the Link-16 model suite. These include the Joint Tactical Information Distribution System (JTIDS) model, the JRE Processor model, and the Link-16 Host model. Each model is shown in a sample Link-16 deployment depicted in Figure 3.

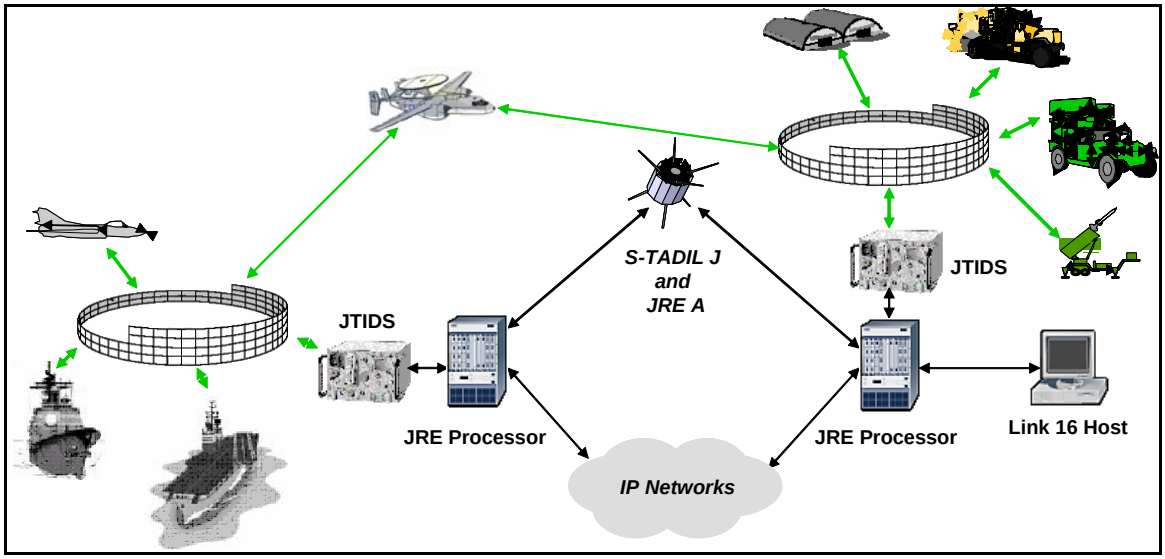


Figure 3. Example Deployment of the Link-16 Model Suite Devices.

The JTIDS device model represents the radio terminal that is used for receiving and transmitting J-series messages within wireless tactical networks. JTIDS terminals provide the wireless interface to a JTIDS network for all Joint participants, including ships, aircraft, and ground assets. The JRE Processor model represents the JRE gateway for Link-16 information. Through the JRE gateway, Link-16 messages may be forwarded over long-haul communications assets such as SATCOM links, voice circuits, and

Internet Protocol (IP) networks. The Link-16 Host model represents the end system for generating and receiving J-series messages. This model may connect to a JRE Processor or a JTIDS model for message forwarding and dissemination. Design features of the three Link-16 models are presented in later sections.

3.3.1 Simulation Environment and Fidelity

The Link-16 model suite is constructed using the Optimized Network Engineering Toolkit (OPNET) and is adapted for use within the NETWARS environment. Models within OPNET/NETWARS are considered *packet*-level models. Packet-level simulations model the transfer of representations of packets among communication devices and protocols. Other levels of communications modeling include the *flow*-level, where messages are aggregated and simulated as flows, and the *bit*-level, where each individual bit of a message is represented as a structure within a simulation. Packet-level models can reach very high levels of fidelity. The Link-16 model suite is no exception, where explicit structures that represent J-series messages, packed transmission frames, and 5-bit pulses are all individually simulated at various levels of framing, encapsulation, and segmentation.

3.4 JTIDS Device Model

The JTIDS device model simulates the radio portion of a local Link-16 wireless network for exchange of tactical J-series messages. JTIDS terminals may be found on a wide variety of Joint assets, where the terminal manages access to a shared broadcast medium among several participants. Figure 4 depicts a sample JTIDS network and illustrates the wide variety of military assets that employ JTIDS terminals.

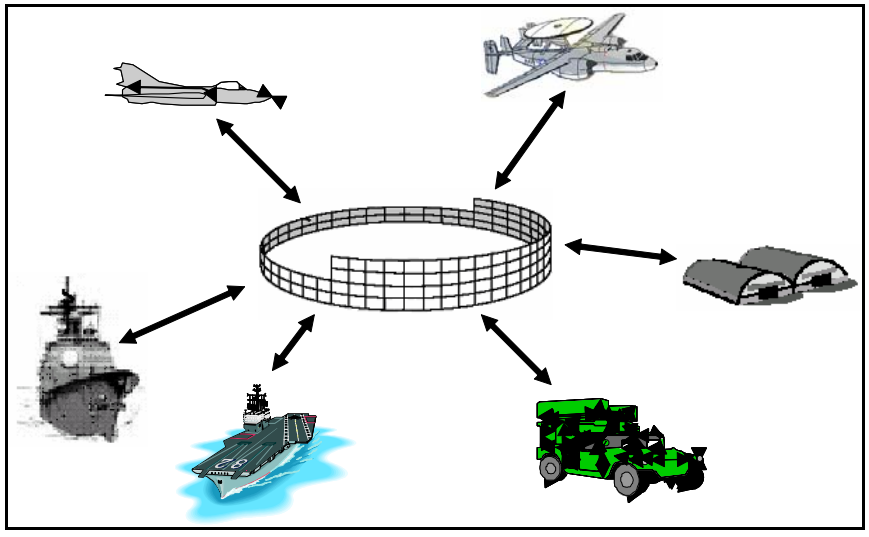


Figure 4. A JTIDS Radio Network.

3.4.1 General Information Flow

Figure 5 illustrates the general flow of J-series message traffic through the JTIDS terminal. JTIDS implements a Time Division Multiple Access (TDMA) based protocol for sharing wireless transmission bandwidth resources among networked terminals. During normal operation, JTIDS terminal models change states among the *transmit*, *receive*, and *idle* states. State transitions occur within fixed time slots, or every 7.8125 milliseconds.

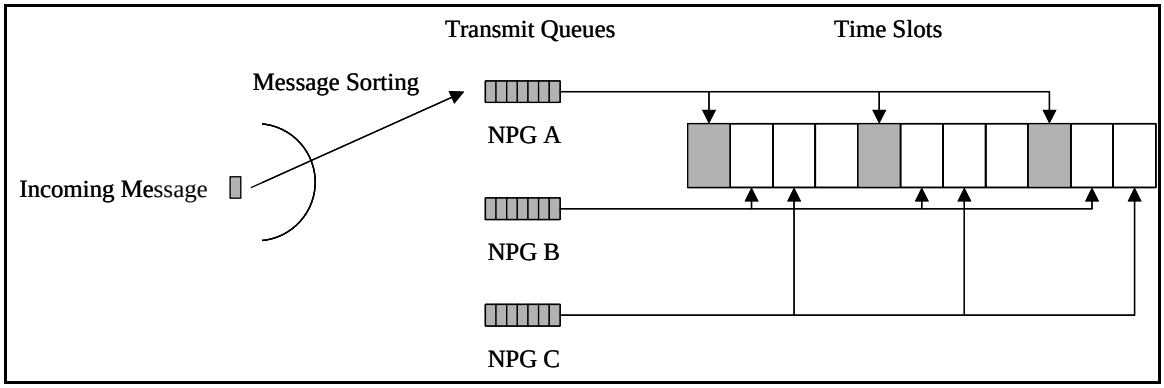


Figure 5. General JTIDS Message Flow Architecture.

The JTIDS model supports Network Participation Groups (NPGs) numbered 0 through 29. NPGs are modeled within the terminal as a combination of logically separate message queues that are associated with sets of transmit and receive time slots. J-series messages are received from local sources and placed into NPG message queues to await transmission. NPG queue assignments for a message are based on message label and sub-label values and the J-series message standard in [9]. Messages are received within receive time slots that are assigned to each respective NPG.

Time slots associated with a particular NPG are organized into Time Slot Blocks (TSBs). A TSB is a set of equally spaced time slots that occur during each complete JTIDS network time cycle, or Epoch. The model supports the assignment of one or more TSBs to a NPG to provide the NPG with time slots that may be used to transmit or receive messages.

3.4.2 Summary of Features

This section identifies the features that the JTIDS model supports. In general, these features comprise the core transmission and reception capability of the JTIDS system. Specific features are listed in Table 1.

Table 1. JTIDS Model Features.

Feature	Description
Time Division Multiple Access (TDMA)	Link-16 implements a Time Division Multiple Access (TDMA) based protocol as described in the previous section.
Network Participation Groups	The Link-16 model supports Network Participation Groups (NPGs) numbered 0 through 29.
Time Slot Blocks	The model supports the assignment of one or more TSBs to a NPG to provide the NPG with time slots that may be used to transmit or receive messages.
Dedicated Access	The access mode for a Link-16 TSB defines the method that is used to gain permission to use the slot for data transmission. The Dedicated access mode is the most commonly used access modes within Joint Network designs. Dedicated access TSBs may be configured for transmission, reception, or relay of data.
Contention Access	Contention access shares a pool of slots among multiple transmitters. Transmit slots are selected randomly from a slot pool, where the maximum number of slots that may be acquired by a transmitter are restricted by a parameterized access rate.
Time Slot Reallocation (TSR)	Time Slot Reallocation (TSR) is a slot-sharing access mode that requires terminals to select slots from a common slot pool as needed. Slot acquisition and negotiations occur once every reallocation period.
Packing Levels	Up to 12 J-series message words may be sent or received within a single time slot, depending on the message packing level. The Link-16 model will implement all four message packing (and pulsing) levels; Standard Double-Pulsed (STD-DP), Packed-2 Double-Pulsed (P2DP), Packed-2 Single-Pulsed (P2SP), and Packed-4 Single Pulsed (P4SP).
Message Receipt Compliance (MRC)	The model supports Message Receipt Compliance (MRC) for a selection of J-series message types.
Network Stacking and Frequency Hopping	The Link-16 model supports the multinetting functionality. Modeled radio transmissions supports frequency hopping and stacked net degradation. Stacked nets may be configured based on Transmission Security (TSEC) or net ID hop patterns.
Error Detection and Correction	Several layers of Link-16 EDAC and encoding are implemented by the model. These include the top-level parity-checking, Reed-Solomon (RS) encoding, and Cyclic Code Shift Keying (CCSK). Each of these data transformations increases the error resiliency of data transmissions.
Wireless Channel	Wireless channel transmission effects include antenna gain, propagation loss, co-channel interference and fading, ambient noise, and radio propagation and transmission delays.

3.5 The Link-16 Host and JRE Processor Device Models

Two processor device models are provided within the Link-16 model suite. The Link-16 Host processor models the end-to-end generation and reception of J-series message traffic through the modeled networks. It collects end-to-end communications statistics and features a flexible user interface to support the rapid reconfiguration of Link-16 message traffic conditions to reflect various simulated scenarios. It supports interfaces to both the JTIDS radio model and the JRE Processor model.

The JRE Processor provides a gateway into a Link-16 network through long-haul media. This gateway is used by remote command and control centers for monitoring Link-16 communications, to connect Beyond Line-of-Sight (BLOS) Link-16 networks, and as a backup for wireless Link-16 communications. Figure 4 illustrates a sample scenario where a JRE Processor model is used to connect two disparate Link-16 networks.

As shown in Figure 6, the JRE Processor model supports several types of interface configurations. It may interface directly with a Link-16 host computer to emulate a Link-16 message transmission and forwarding system. It also interfaces directly with JTIDS radios to emulate a tactical host system. In addition, it supports many types of JRE processor-to-processor Link-16 communications through long-haul media. This includes message exchange through broadcast SATCOM systems such as UHF Demand Assigned Multiple Access (DAMA), and through all types of Internet Protocol (IP) networks.

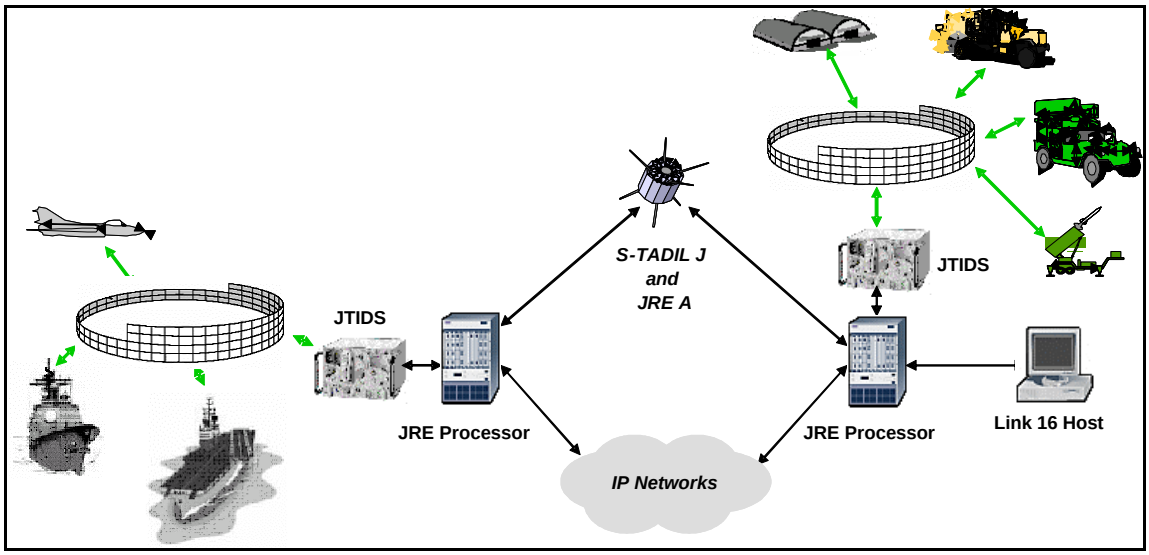


Figure 6. A JRE Processor Network.

The centerpiece of the JRE Processor model is the implementation of the JREAP specification. JREAP, based on MIL-STD-3011 [10], defines the protocols that are used for transmission of Link-16 data over different types of long-haul media. It includes

specifications for J-series message encapsulation and fragmentation, and management message traffic (such as peer-to-peer updates).

Three types of JREAP protocols are included within the MIL-STD-3011 specification. These include JREAP A, JREAP B, and JREAP C. JREAP B, which specifies Link-16 communications through point-to-point JRE media such as dial-up voice circuits, is not supported by the JRE Processor model. JREAP A specifies communications through broadcast SATCOM networks, such as EHF MilStar and UHF DAMA. JREAP A is under development in support of the NETWARS Link-16 model standardization effort. JREAP C, which is currently supported by the JRE processor model, defines the Link-16 standard for communications over IP-based networks.

In addition to encapsulation that allows Link-16 messages to be incorporated into protocol packets, the JREAP C process models the effects of packet segmentation and reassembly, and management traffic. Management traffic includes JRE Processor peer-to-peer traffic such as Direct Connection List updates, Connectivity Feedback, and Network Connectivity Matrix updates. Modeling of management traffic is an important capability of the JREAP model, as management traffic impacts network congestion levels.

4.0 Knowledge Superiority and Assurance (KSA) Future Naval Capability (FNC)

Our M&S efforts supporting Knowledge Superiority and Assurance (KSA) Future Naval Capability (FNC) projects sponsored by Office of Naval Research (ONR) are highlighted by the following two selected studies. The first [11] illustrates the use of M&S to examine ways of constructing a single worldwide 300-ship Navy network that supports ship-to-shore communications. The second effort [12, 13] involves simulation-assisted routing design for integration of JTRS-like radios, such as the VRC-99 A/B, into Naval data networks. These two studies reiterate the utility of M&S in assessing competing network designs under conditions that would have been prohibitively expensive to create in the lab or in the field. The M&S tool QualNet for communication networks was used in both efforts.

4.1 Toward a Unified Naval Network

The advantages of a single routing domain include transferring more of the maintenance from humans to network devices, while at the same time improving reliability. The expected result of a unified routing domain is that network maintenance will require tens or hundreds fewer personnel, while at the same time reducing network outages between ships and shore sites.

There are two crucial issues encountered in constructing a unified Naval network: limited bandwidth and scalability. Currently, most Navy ship-to-shore links are based on geosynchronous satellite communications (SATCOM). Limited bandwidth on the SATCOM links is a significant problem. Therefore, this M&S effort looked for routing architectures that can be implemented within limited bandwidth environments. On the

other hand, the primary goal of this endeavor was to examine network architectures that might be able to scale to a 300-ship worldwide routing domain.

Two routing architectures were considered. One was the current Open Shortest Path First (OSPF) design [14] extended to a single worldwide routing domain. The second was an architecture developed as part of the KSA FNC Traffic Flow Engineering (TFE) project sponsored by ONR [15].

4.1.1 Current Network Architecture

The current ship-to-shore architecture is based on the OSPF routing protocol. A key feature of OSPF is that it requires all routers in an area to have complete routing topology information for that area. OSPF ensures complete knowledge by first flooding all advertisements throughout the area as routers join the network. OSPF then floods all advertisements throughout the area every 30 minutes [14], in order to continually refresh the link state database. Finally, OSPF floods specific advertisements when link status changes (link up or link down).

Distributing this information can lead to significant bandwidth consumption because every router needs the same information. If there are N routers in an area, then each router must send its advertisements to N-1 other routers. The total number of transmissions grows on the order of N(N-1), or approximately N^2 transmissions. Exponential growth means the routing protocol overhead grows rapidly as the number of routers in an area increase.

The traditional way to control OSPF bandwidth consumption is to limit the number of routers in each area. In the Navy's case, all the ship-to-shore networks are in one area, area zero (the OSPF backbone). This means the traditional way to limit OSPF bandwidth consumption is to limit the number of ships in the ship-to-shore network. This has led to multiple ship-to-shore routing domains, one each in the Atlantic, Pacific, Mediterranean, and Indian Ocean Regions.

4.1.2 Proposed Traffic Flow Engineering (TFE) Architecture

The Traffic Flow Engineering (TFE) architecture approach to scaling the network relies on features of the Enhanced Interior Gateway Routing Protocol (EIGRP) [16]. In contrast to OSPF, the EIGRP protocol (like other distance vector routing protocols) does not require complete routing information. This, in turn, allows EIGRP to accommodate arbitrary information hiding. This information hiding can be used by the Navy to reduce routing protocol overhead, and thereby enhance network scalability.

Two salient features of the TFE architecture are its uses of EIGRP router filters and query boundaries to enable scalability.

Router Filters: The TFE architecture uses EIGRP route filters to limit routing protocol on the ship-to-shore links. Figure 7 illustrates the placement of these filters. The filters limit

routing protocol by allowing it to flow from ship-to-shore, while preventing it from flowing over the SATCOM links back toward the ships.

Query Boundaries: Excessive queries are also a matter of concern because they can use considerable bandwidth. Queries occur when an EIGRP router loses a path to a specific network and has no other loop-free path. The router responds to the loss by asking neighboring routers for an alternate path. This is a potential problem because, in some cases, the query might propagate throughout the entire network. The TFE architecture minimizes the query problem by implementing query boundaries. These boundaries are implemented using the same route filters shown in Figure 7.

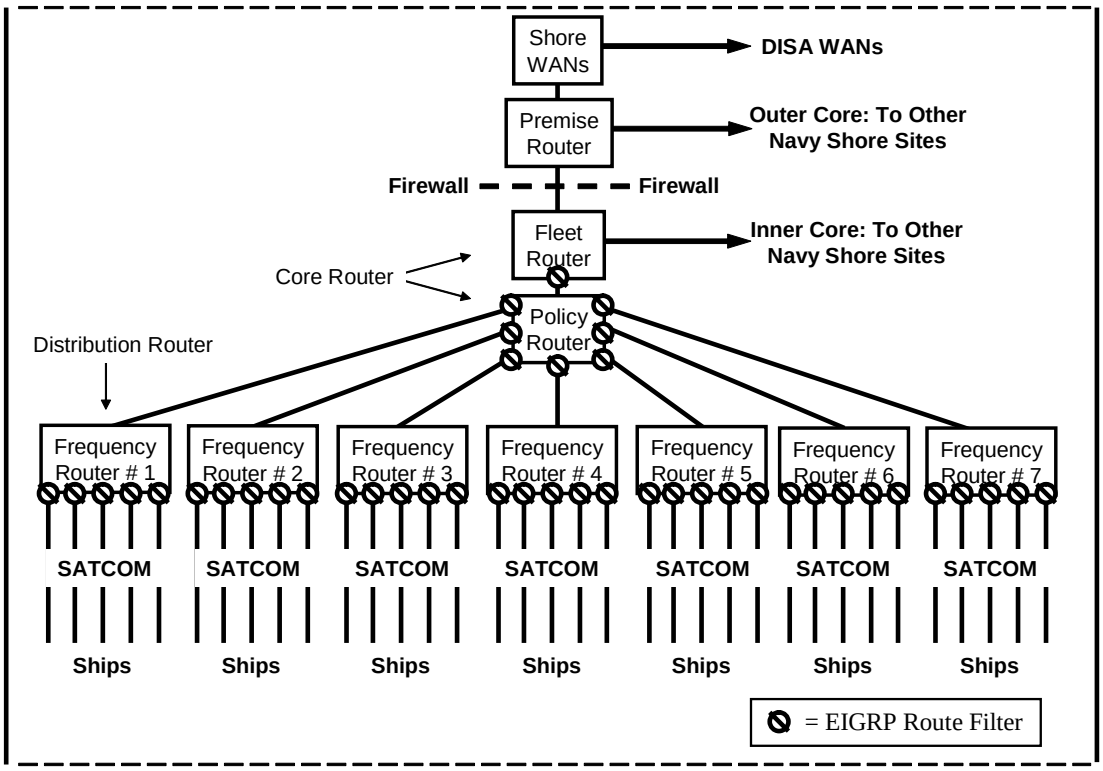


Figure 7: Placement of Route Filters within a Navy Shore Site.

4.1.3. Simulation Results

A single worldwide naval autonomous system with 300-ships was modeled using the M&S tool QualNet. A summary of our simulation results is presented here where extensive results of the study can be found in [11].

OSPF Bandwidth Consumption: A striking result of these simulations was the predicted effect of satellite link failures on the OSPF protocol. In a worldwide 300 ship Naval network, bandwidth consumption was minimal (about 400 bits per second per satellite link) until link failures were introduced. In the presence of link failures, the OSPF routing

protocol was predicted to consume between 1,000 and 10,000 bits per second (bps) on each satellite link.

TFE Bandwidth Consumption: This simulation predicted bandwidth consumption for the TFE architecture under the network conditions used to test OSPF, except that the routers were configured to run EIGRP according to the TFE architecture. Under these conditions, the EIGRP routing protocol used less than 100 bits per second (bps), and were relatively unaffected by link failure.

Figure 8 compares the OSPF and EIGRP data in the presence of link failures. Note that the Y-axis is logarithmic. A difference of 2 Log_{10} units indicates a 100-fold difference in bandwidth consumption.

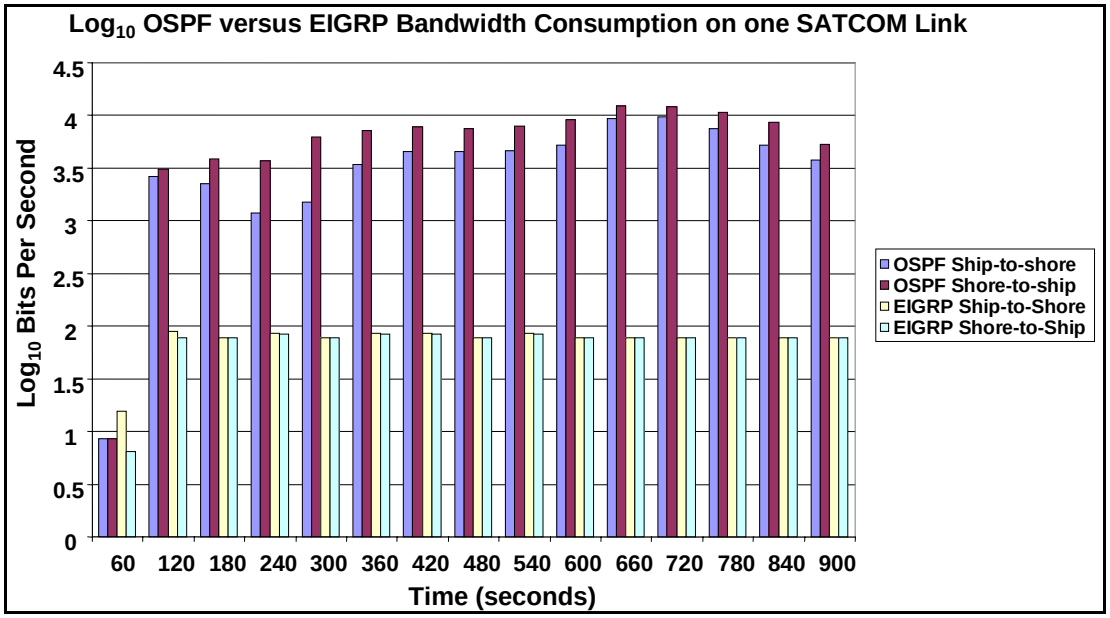


Figure 8: A Log_{10} Comparison of OSPF and EIGRP Bandwidth Consumption.

Throughout Figure 8, the EIGRP traffic is consistently less than 2 Log_{10} units. This represents a little less than 100 bps on this satellite link. The OSPF data ranges from 3 to 4 Log_{10} units, or between 1,000 and 10,000 bps, on the same satellite link. The difference is 1 to 2 Log_{10} units, or 10 to 100 times more OSPF traffic. The maximum differences occurred during the 660 and 720 second periods, where the difference is more than 2 Log_{10} units, i.e., OSPF used more than 100 times more bandwidth than EIGRP.

The major result was that the TFE architecture was predicted to consume less than 100 bps per SATCOM link, even if each individual satellite link failed every 22.5 minutes – this link failure rate is a reasonable first approximation confirmed by an Operation Iraqi Freedom (OIF) Lessons Learned White Paper [17] and data recorded during the FORCEnet Initial Product Demonstration (IPD) in September 2003. By contrast, an OSPF-based network exhibited significant amounts of routing protocol traffic, and it is

predicted that the OSPF-based design tested here would not scale well to a worldwide Naval network.

4.2 Simulation-Assisted Routing Protocol Design

The Simulation Modeling and Analysis for Naval Battleforce Network (NBN) effort supports communications technology developers at Space and Naval Warfare Systems Center San Diego (SSC San Diego), and, in particular, the Intra Battle Group Wireless Networking (IBGWN) project of the ONR Naval Battleforce Network (that is part of KSA FCN). The NBN program goals include better adaptive, mobile, wireless networks connecting multiple Naval platforms within a battle group, as well as joint battlefield scenarios. In this case, our M&S effort supports integration of Joint Tactical Radio System (JTRS)-like radios, such as the VRC-99A/B, in Naval data networks.

An interesting problem, namely the subnet-relay problem, occurs in line-of-sight and beyond-line-of-sight (LOS/BLOS) networking radios. The IP Subnet model requires that the link layer allow any IP device to send a packet directly to any other IP device on that subnet (see [18], page 2). However, limited radio range, combined with mobility of nodes, means wireless networks do not always comply with the IP Subnet model. In fact, LOS/BLOS radios often require dynamic relaying between nodes as the need for, and location of, the relays can change frequently. Thus, the subnet-relay problem is central to integrating LOS/BLOS radios into larger IP data networks.

Various solutions have been tested. Originally, physical implementations were developed and tested in field trials. However, these efforts were time consuming and expensive. In an effort to reduce risk and cost, a number of efforts are under way to use Simulation-Assisted Design in order to test the performance of routing protocols, before going to field trials of proposed subnet-relay solutions.

Open Shortest Path First (OSPF) Point-to-Multipoint mode can solve the subnet-relay problem, but a previous simulation study [19] found this mode to be poorly suited to typical military LOS/BLOS networks. In our simulation-assisted protocol design study [12, 13] we examined a different solution to the subnet-relay problem. The goal was to have the radios emulate the IP subnet model, based on dynamic link-layer routing.

4.2.1 Protocol Design and Description

The design used Layer 2 routing based on Ethernet addresses. The potential advantages of Layer 2 routing are 1) it is easy to implement, and 2) the resulting wireless network integrates well into larger IP networks. The appearance of a standard IP subnet allows virtually any COTS router to be used with the networking radios. It also allows the routers to run any routing protocol over the networking radios.

The general architecture is illustrated in Figure 9. For any given IP/Ethernet packet, the radio will always see a router Ethernet address as the source and the Ethernet address of

another subnet router, or a broadcast/multicast address, as the destination. This invariance is the basis of this routing proposal.

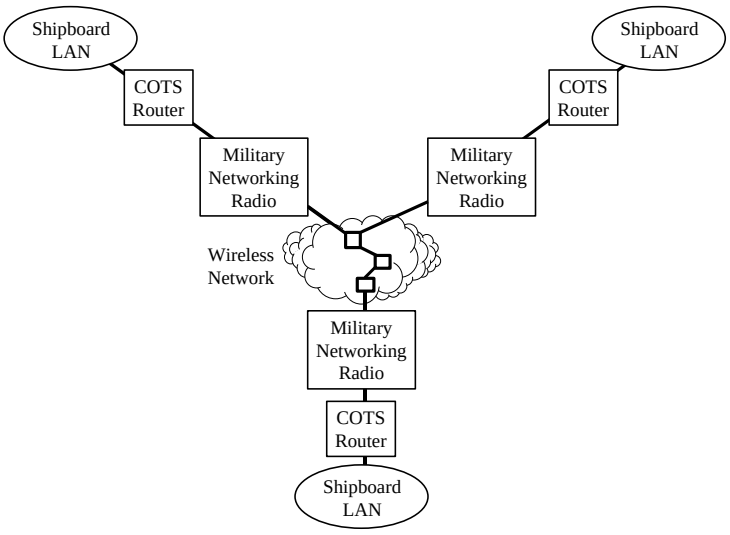


Figure 9: Physical Relationship of Routers and Networking Radios.

The intention of this design is that the cost of each link be defined by the link layer (Layer 2). In the case of the VRC-99, the link layer continuously adjusts the link bandwidth to each neighboring radio based on receipt of link connectivity packets. The link layer then assigns a routing protocol cost. In the current simulation, the link costs were manually assigned

Each radio used periodic, unreliable, broadcast of topology data to distribute the link-state data. Furthermore, each radio's link state broadcast incorporated all link state data received from other radios, as well as its own information. In the study, various numbers of nodes, i.e., from 4 to 16 nodes, and various update periods were used, i.e., from once every 10 seconds to once per second.

4.2.2. Simulation Results

The simulation-assisted routing protocol design was performed using the M&S software tool QualNet. The performance of the proposed routing protocol was measured in terms of the protocol bandwidth consumption and the speed of convergence.

We present a summary of the study's results here; more results and detailed discussion of the design can be found in [12, 13].

Bandwidth Consumption: To measure protocol bandwidth consumption, the amount of bandwidth used by the Layer 2 (subnet-relay) routing protocol was measured. The protocol sent the entire connectivity matrix inside every routing protocol update and the size of the matrix varied depending on the number of nodes in the subnet. Note that for

the VRC-99, the link connectivity packet (which communicates link sate information) is 144 bytes long regardless of the number of radios in the network. The 144-byte size includes the packet header and all but 12 bytes of slot overhead.

Test 1: The update rate remained constant at 1 routing protocol packet per second per node but the number of nodes varied. As seen in Figure 10, bandwidth utilization increased as the number of nodes in the connectivity matrix increased. Four nodes consumed about 500 bits per second per node. Sixteen nodes consumed about 5,000 bits per second per node. The rate of increase in bandwidth consumption was on the order of N^2, where N is the number of nodes in the connectivity matrix. Bandwidth consumption increased rapidly because the connectivity matrix is two dimensional and is contained in all routing protocol packets.

Test 2: The number of nodes remained constant at 10, but the update interval varied. The amount of bandwidth consumed increased as the update interval increased as seen in Figure 11. Update intervals of 1, 2, 4, 6, 8, and 10 seconds were tested. When the update interval was once every 10 seconds, the protocol consumed about 500 bits per second per node. When the update interval was once per second, the protocol consumed about 5,000 bits per second per node.

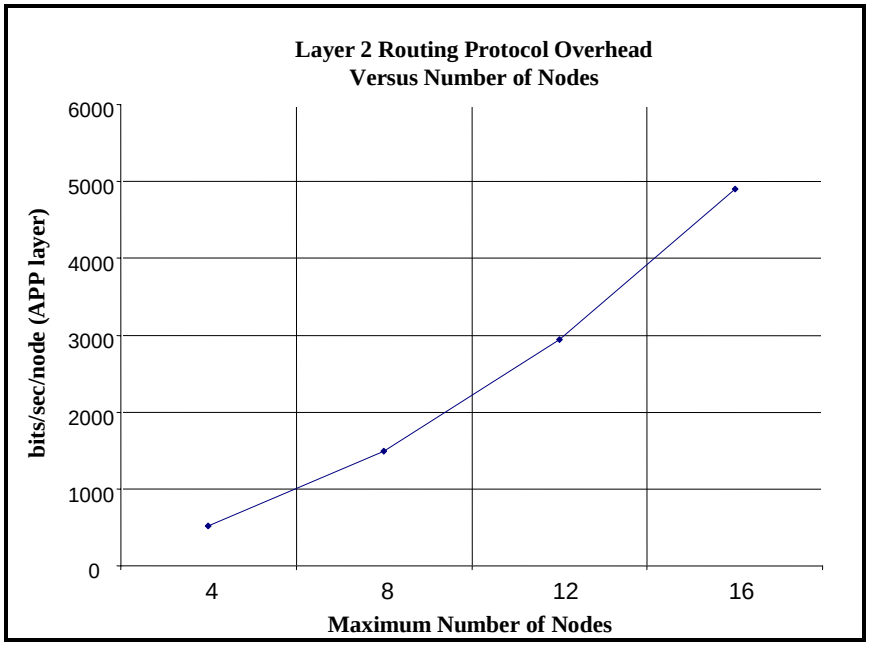


Figure 10: Protocol Overhead Versus Number of Nodes.

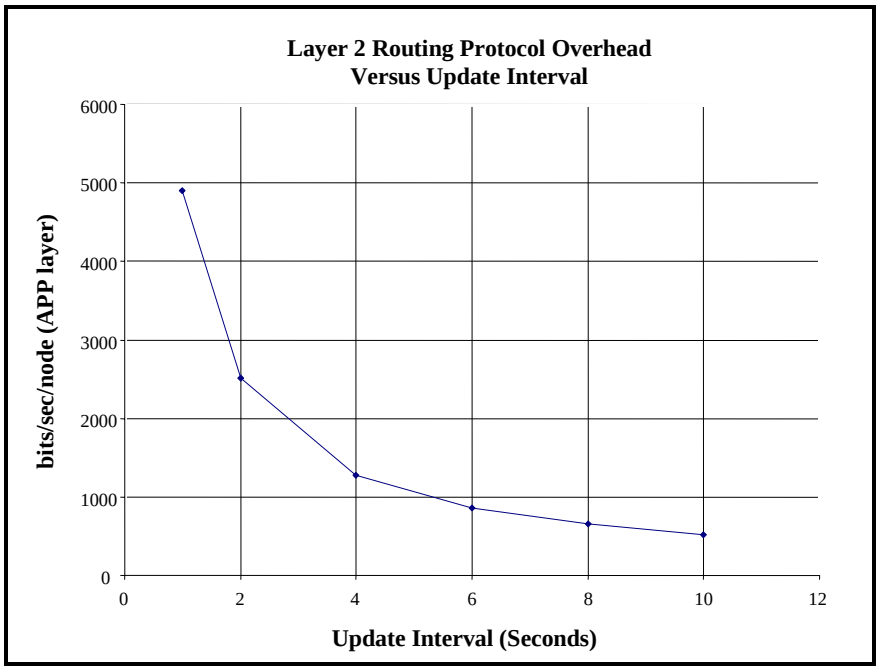


Figure 11: Protocol Overhead Versus Update Interval.

Speed of Convergence: The effect of mobility on the speed of convergence was a central concern. Based on radio range calculations, it was possible, in some scenarios, to calculate the time difference between a node coming into radio range and the time the first application packet was received by that node. This time difference was used as the definition of routing protocol convergence.

Test 3: During the first 100 seconds, all nodes were within radio range of all other nodes. The first application packet was received by all nodes, indicating the protocol converged immediately after the first routing protocol packet was sent. At time 100, all nodes moved out of radio range of all other nodes. Between 14 and 17 seconds after the movement, the routing protocol formally declared all neighbors lost and all routes invalid. At time 200, all nodes moved back to within radio range of all other nodes. Application packets were received immediately after the next routing protocol packet, indicating the protocol again converged immediately.

In other mobility scenarios, convergence took longer. The exact pattern of node movement determined the length of time to converge. Some patterns led to rapidly changing patterns of physical connectivity, in these cases, and convergence took longer.

In general, this extremely simple routing protocol was able to facilitate the delivery of end-user (application) packets. The protocol should be relatively simple to implement. Furthermore, the independence of the subnet-relay routing algorithm from the routing protocol used by the larger network means any manufacturer and any routing protocol can be used.

5.0 Related Efforts

SSC San Diego Network Centric Warfare Analysis Branch also initiates and engages in several efforts to support and complement a full spectrum of M&S environments. One of these endeavors is the DARPA-funded Non-Intrusive Knowledge Suite for monitoring network and application performance. Another noteworthy ongoing activity is our lab and field experiment in support of FORCEnet and the Joint Rapid Architecture Experiment (JRAE).

5.1 Non-Intrusive Knowledge Suite (NIKS)

One of the observations emerging from our branch's M&S initiatives is that accurate and standardized datasets of network performance are needed to perform Verification, Validation, and Accreditation (VV&A) of M&S programs. Additionally, the operational and tactical community has expressed a desire to have such datasets available, in as close to real-time as possible, to diagnose operational networks and systems.

Accordingly, our branch is leading the development of state-of-the-art methods and products for monitoring network and application performance in a non-intrusive manner. The latest product to emerge from this initiative is the Non-Intrusive Knowledge Suite (NIKS). The NIKS was developed by the Cooperative Association for Internet Data Analysis (CAIDA, www.caida.org), under the direction of our branch that served as the government Technical Agent for the DARPA Network Modeling and Simulation (NMS) program. Additional support has been generously provided by the Reconfigurable Land Based Test Site (RLBTS) ShadowLab at SSC San Diego in the form of application testing opportunities, and continued encouragement and good will.

The NIKS operates on the tcpdump (www.tcpdump.org) and CAIDA's CoralReef [20] software stacks. The main advances offered by NIKS beyond these products are to be found in the crl_delay module. This module records the one-way latency of each packet between two ethernet ports when both ports see the same packet, as well as the latency or "TCP Round Trip Time" (TCPRTT) for all Transmission Control Protocol (TCP) packets at any one ethernet port, and outputs this and related information such as source and destination IP addresses and ports, sequence number, and packet lengths, in real-time or nearly so. One line of output per packet, or about 100 bytes, is adequate to report this information. At the end of each crl_delay run, all relevant numbers (e.g., connection start time, connection duration, number of packets during connection) and derived statistics of latencies are tabulated for each TCP connection observed as open during the run. This tabulation can be referred to as crl _delay "End Of Run Statistics" (EORS), from which many useful conclusions about the functioning of applications over the Wide Area Network (WAN) can be deduced. Similar information for packets of other protocols observed such as the User Datagram Protocol (UDP) or the Internet Control Message Protocol (ICMP) are also recorded, in real time and as EORS.

The crl_delay module is also capable of working on more than two interfaces, and this multi-interface capability can be used, in principle, on remote Linux platforms collecting single-interface information simultaneously, using CoralReef's crl_to_pcap suite for example. For the best information of course, the clocks on the various platforms must be synchronized using GPS or an equivalent protocol. Failing that, the crl_delay latency calculations, that are performed after crl_to_pcap archiving, will inherently include the offset time (or delta time) between two platforms, and therefore will be subject to interpretation error.

Since operational systems are not necessarily able to incorporate precise time protocols such as GPS, current work is focusing on a potentially high-reward extension of NIKS to post-process data from a remotely distributed network of NIKS platforms, and to compensate in various ways for asynchronization of platform clocks by regression analysis of one-way raw packet delays, additionally using the TCPRTTs as checks on such analysis.

5.2 Lab and field experimentation

In addition to computer-based modeling and simulation, we are active in lab-based and field experimentation efforts, particularly those associated with the Navy's FORCEnet initiative. These experimentation efforts complement our software-based experimentation, providing evidence for VV&A and enabling studies with greater focus on operational environmental factors and Human Systems Integration (HSI).

5.2.1 Metrics

As with modeling and simulation, lab and field experiments start with the definition of clear experiment objectives. Generally our studies involve installing and integrating many systems together, requiring objectives addressing entire packages of systems, though system-level objectives are often included as well.

Once the objectives are clearly defined, they are further broken down into analysis questions, usually several for each objective, that help to describe the objective in more practical terms.

Analysis questions are further expanded into measures of effectiveness (MOEs), then measures of performance (MOPs) from which we can determine the actual data collection requirements. Figure 12 shows the data collection taxonomy of experiment objectives, analysis questions, MOEs, and MOPs.

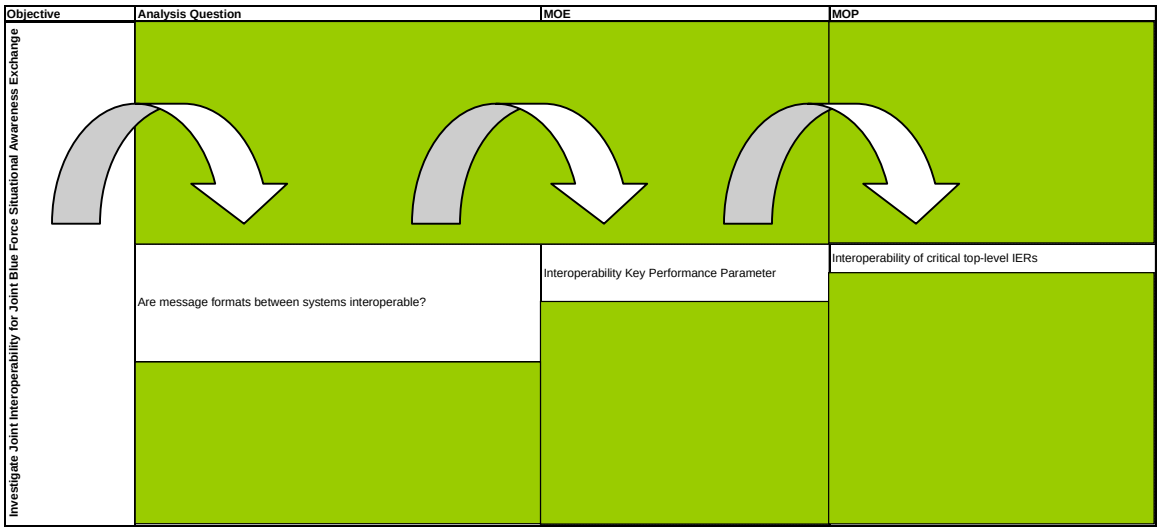


Figure 12. Data collection taxonomy.

5.2.2 Replication of network and applications

When the experiment objectives are clearly articulated, we can architect the system components that need to be installed in the laboratory. As in software-based modeling and simulation, there is often a trade-off between fidelity and expense or time. The experiment objectives allow us to determine where high fidelity is required and where lower fidelity is acceptable. For instance, interoperability of systems is sometimes largely independent of the network connecting them, making hard-wire connections between systems an acceptable replication. In other cases, the network itself affects the system interoperability, requiring a higher fidelity replication of the network in the lab. Where high fidelity replication is required, we install and use the same equipment (hardware, software loads, etc.) that will be deployed for military use, if feasible.

In many cases, it is not possible to locate all the systems in one lab, requiring distributed experimentation among two or more labs. Networks such as the Defense Research Engineering Network (DREN), Secure Internet Protocol Router Network (SIPRNET), or the Internet can provide connectivity between labs (though there are often restrictions on running experiment traffic across some of these networks). Though it complicates experiment design, distributed experimentation is often a better representation of the way systems will actually be fielded.

In field experimentation, replication is normally not an issue, though it may be necessary to restrict the use of legacy systems in order to conduct adequate tests. It can also be difficult to ensure appropriate network traffic is generated in an exercise environment.

5.2.3 Data collection

The metrics derived from the overarching experiment objectives dictate what data collection is required. Some data can be collected directly from systems, through items such as system logs or message logs. Some data is collected by observers keeping logs of events. In some cases, questionnaires are constructed to be completed by certain experiment participants. Other data requires the use of special instrumentation such as network sniffers or network monitoring software.

5.2.4 Experiment execution

During the execution of the laboratory and field experiments, analysts monitor collection devices and determine if the data being collected is adequate. They often administer questionnaires or conduct interviews with system operators for HSI metrics. They also ensure that data is archived in appropriate formats to enable expeditious analysis.

5.2.5 Analysis

Following experiment execution, analysts typically are called on to produce a quick look report, then a final report. Data is reviewed for validity and analyzed to determine the MOPs and MOEs. With this supporting evidence the analysis questions can be answered and the overall experiment objectives assessed.

5.2.6 Summary

Combining software-based M&S with lab and field experimentation has been very beneficial to the Network Centric Warfare Analysis Branch. M&S can highlight areas of study for lab and field experimentation and can assist in areas where lab and field experimentation is limited, such as scalability and Monte-Carlo type repetition. Laboratory experiments can help to validate software models and provide a means for relatively easy data collection. Field experiments are another source for model validation, usually allowing the highest fidelity analysis at the expense of high cost.

Having these experimentation capabilities in one facility enables valuable collaboration among analysts. Recently, a particular routing protocol was analyzed using software-based M&S with commonly assumed SATCOM outage rates. Field experiments revealed that actual SATCOM outage rates differed substantially from the assumptions. The routing protocol model was run again using the different outage rates obtained from field experiments, and yielded significantly different results. The collaboration made possible by the close partnership of analysts and modelers led to more accurate results and better analysis.

6.0 Conclusion

Making use of the full spectrum of modeling and simulation environments is one of the key activities for Network Centric Warfare Analysis. Fundamental to our branch operations is the development of standard, reusable, interoperable models to reduce cost and enhance model assessment time. We work with all facets of the M&S community,

which includes Joint Services, government agencies, deployed operational commands, academia and industry in order to support the Navy with the best possible analytical capability. We continue to enhance our capability by working with the Department of Defense High Performance Computing Modernization Office (HPCMO) to support simulation runtime performance, DARPA Network Modeling and Simulation (NMS) program office to leverage new technologies in M&S, DMSO and NAVMSMO to support policy, standards and guidance. Our capabilities are evolving with technologies to support the Navy and extend to satisfy Joint and Coalition operations.

References

[1] NETWARS Program Management Office. *NETWARS User's Guide Release 2002-2*. Defense Information Systems Agency (DISA), December 2002.

[2] Space and Naval Warfare Systems Center San Diego. *Space and Naval Warfare Systems Center Navy Communications Device Conversion Effort V&V Report*. SPAWARSYSCEN San Diego, January 2003.

[3] T. Hepner, C. Alspaugh, C. Tran, and W. Youm. *Space and Naval Warfare Systems Center Navy Communications Device Conversion Effort V&V Report*. SPAWARSYSCEN San Diego, February 2004.

[4] C. Alspaugh, T. Hepner, C. Tran, W. Youm, A. Legaspi, S. Ferenci, R. Fujimoto, and M. Choi. "Navy NETWARS Interoperability Efforts," Paper 04S-SIW-93, 2004 Spring Simulation Interoperability Workshop, Simulation Interoperability Standards Organization (SISO), Arlington, VA, 18-23 April 2004.

[5] W. Stevens, J. Jones, and J. Monroe: *NSS v3.3 Analyst Guide*, prepared by Metron, Inc. for Space and Naval Warfare Systems Command (SPAWARSYSCOM) PMW-153, August 2002.

[6] D. Carr and C. Maru: *NETWARS Model Development Guide Version 1.6*, prepared by OPNET Technologies, Inc. for Defense Information Systems Agency (DISA), December 2003.

[7] Navy Center for Tactical Systems Interoperability (NCTSI). *Understanding Link 16 – A Guidebook for Operators, Technicians, and Net Managers.* September 2001.

[8] C. Alspaugh and A. Legaspi. "A Violation of Order: IP-QoS for Tactical Traffic," Proceedings of MILCOM 2002, Anaheim, CA, 7-10 October 2002, Vol. 2, pp. 1275-1280.

[9] Department of Defense. *Department of Defense Interface Standard – Tactical Digital Information Link (TADIL) J*. MIL-STD-6016A, 7 February 1997.

[10] Department of Defense. Department of Defense Interface Standard – Joint Range Extension Application Protocol (JREAP). MIL-STD-3011, 30 September 2002.

[11] M. Stell, C. Tran, and A. Legaspi. "Toward a Unified World-Wide Navy Network," Paper 04S-SIW-089, 2004 Spring Simulation Interoperability Workshop, Simulation Interoperability Standards Organization (SISO), Arlington, VA, 18-23 April 2004.

[12] M. Stell, C. Tran, and A. Legaspi. "Simulation-Assisted Routing Protocol Design (SARPD)," Paper 03F-SIW-127, 2003 Fall Simulation Interoperability Workshop, Simulation Interoperability Standards Organization (SISO), Orlando, FL, 14-19 September 2003.

[13] M. Stell, C. Tran, and A. Legaspi. "Case Study: Designing a Wireless Routing Protocol," Presentation at QualNet World 2003, Boston, MA, 15-17 October 2003.

[14] J. Moy. *OSPF Version 2*. STD 54, RFC 2328, April 1998.

[15] B. Chan, D. Leung, E. Otte, and K. Owens. *Fleetnet 2.0 A Prototype IP Routing Architecture for the Fleet*. SPAWARSYSCEN San Diego, 13 November 2002.

[16] I. Pepelnjak. *EIGRP Network Design Solutions*. Cisco Press, Indianapolis, IN, 2000.

[17] CAPT P. Baumann, USN. *Operation Iraqi Freedom (OIF) PEO C4I and Space Lessons Learned White Paper*. U.S. Navy PEO C4I and Space, 9 July 2003.

[18] Y. Rekhter, D. Kandlur: "Local/Remote Forwarding Decision in Switched Data Link Subnetworks," RFC 1937, May 1996.

[19] T. Henderson, P. Spagnolo, and J. Kim: "A Wireless Interface Type for OSPF," Proceedings of MILCOM 2003, 13-16 October 2003, Boston, MA, Vol. 2, pp. 1256-1261.

[20] The Cooperative Association for Internet Data Analysis (CAIDA). *CoralReef*. http://www.caida.org/tools/measurement/coralreef/

Author Biographies

CHRIS ALSPAUGH is an Electrical Engineer at the Space and Naval Warfare Systems Center, San Diego (SSC San Diego). He is the lead engineer for the development of OPNET and NETWARS models at SSC San Diego. He holds a B.S. in Electrical Engineering from the University of California, San Diego (UCSD). He is a member of the NETWARS Architecture & Standards (A&S) WIPT, and the NETWARS Requirements WIPT.

NIKHL DAVÉ, Ph.D. has Bachelor's of Arts Degrees in Physics and Mathematics from University of California at San Diego (UCSD), as well as Masters' in Science, Engineering and Physics, and the Ph.D. in Engineering Physics from UCSD. He has over nineteen years of experience in tactical systems engineering for the DOD, and recently has guided the development of a suite of tools for the characterization of network traffic, loading, and performance. He serves as a Technical Advisor to US Navy N6M.

THOMAS A. HEPNER is a Computer Scientist at the Space and Naval Warfare (SPAWAR) Systems Center in San Diego, CA. He is currently the program manager for the Navy's NETWARS effort. He holds a B.S. and M.S. in Computer Science and Artificial Intelligence from San Diego State University (SDSU). He is a member of the NETWARS Architecture & Standards (A&S) WIPT, the NETWARS Requirements WIPT, and the NETWARS CM, Testing and V&V WIPT.

ANDY LEIDY is an engineer at SPAWAR Systems Center, San Diego. He received his Bachelor's of Aerospace Engineering degree in 1990 from Georgia Tech and was an F-14 Radar Intercept Officer in the U.S. Navy for nine years. His previous experience includes conducting AGM-88 HARM missile aircrew training and managing the design and manufacture of electronic components for the F-22 and other tactical aircraft. His current work focuses on analysis efforts supporting FORCEnet and Joint interoperability experimentation.

MARK STELL, Ph.D. is a network engineer at SPAWARSYSCEN San Diego. For eight years he was a member of the Navy's Automated Digital Network System (ADNS) network design team. His current focus is developing simulation environments to support advanced development of military data communications devices.

CAM TRAN, Ph.D. (Math, UCSD 1988) is a scientist at SPAWAR Systems Center San Diego. He is currently developing communications device models and Operational Facilities (OPFACs) for the Navy's NETWARS effort. He is a member of the NETWARS Architecture & Standards (A&S) WIPT, the NETWARS Requirements WIPT, and the NETWARS CM, Testing and V&V WIPT.

HEATHER WOODS is a scientist at SPAWAR Systems Center, San Diego. She received her Bachelor's degree in Mathematics from Providence College in 2000 and her Master's degree in Mathematics from Boston College in 2002. Her current work has focused on data analysis efforts supporting FORCEnet and Joint Interoperability experimentation. In addition, she has visited two NCTAMS (Naval Computer Telecommunications Area Master Station) facilities to discuss common procedures utilized at these sites along with network management techniques.

WONITA YOUM is an Electrical Engineer at the Space and Naval Warfare (SPAWAR) Systems Center in San Diego, CA. She currently builds organization models for Naval networks, and develops model animations for various projects. She holds a B.S. in Electrical Engineering from the University of Washington. She is a member of the NETWARS Architecture & Standards (A&S) WIPT.

ALBERT K. LEGASPI, Ph.D. (EE, UCSD 1996) is an electrical engineer at SPAWAR Systems Center San Diego. He is currently supporting the Navy Modeling and Simulation Management Office (NAVMSMO) on NETWARS/NSS Federation. Dr. Legaspi is the head of SPAWAR Systems Center San Diego Network Centric Warfare Analysis Branch, and a former Chair of IEEE Communications Society in San Diego, CA.

JIM WEATHERLY currently performs as the Assistant Director of the Navy Modeling and Simulation Management Office (NAVMSMO) at OPNAV N61MB. He has performed as a Research Fellow for the Potomac Institute for Policy Studies; Director for the Department of Navy Modeling and Simulation Technical Support Group (DONMS-TSG), and Deputy Director, NAVMSMO, for the Chief of Naval Operations, OPNAV. He has also performed as Head of the Engineering Support and Integrated Assessment Environment Division, Supervisory Electronics Engineer within the Warfare Systems Architecture and Engineering Directorate (WSA&E), and Head of the Test Facilities Section within the WSA&E Directorate.

SPAWAR
Systems Center
San Diego

Modeling and Simulation in Support of Network Centric Warfare Analysis

SPAWAR Systems Center (SPAWARSYSCEN) San Diego
Network Centric Warfare Analysis Branch
San Diego, CA 92152-5001
Chris Alspaugh, Dr. Nikhil Davé, Tom Hepner, Andy Leidy, Dr. Mark Stell, Dr. Cam Tran, Heather Woods, Wonita Youm, and Dr. Albert K. Legaspi

Navy Modeling and Simulation Management Office (NAVMSMO)
OPNAV N61F21
Washington, D.C. 20350-2000
Jim Weatherly

2004 Command and Control Research and Technology Symposium
15-17 June 2004 – Loews Coronado Bay Resort, San Diego, CA

CCRP

SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

SPAWAR
Systems Center
San Diego

Background

Who We Are

- SSC-SD 2822 (Network Centric Warfare Analysis Branch)
- Represent Navy Modeling and Simulation Management Office (NAVMSMO), OPNAV N61-M, and N61F, for Joint C4ISR Communication M&S assessment domain
- Supporting Communication M&S for 10 years
- Lead Navy NETWARS developers

What We Do

- Perform C4ISR communication system performance analyses
  - Modeling and Simulation (M&S) is our most commonly used assessment method

SPAWAR
Systems Center
San Diego

Communications System M&S Applications

Capacity Planning/Scalability

- Where are my network bottlenecks?
- How will my network support future growth?

Technology Impact

- How will my new application impact existing systems?
- Impact of NBC attacks on network performance?

Acquisition

- Why is this new router better for my network?

Prototype development and assessment

- Before it is deployed, what are the deficiencies in my new TDMA protocol?

SPAWAR
Systems Center
San Diego

Communications System M&S Applications (continued)

Operational Decision Aids/Doctrine Development

- JTF OPTASK COMMS development guidance.

SPAWAR Systems Center San Diego

SSC-SD M&S Capabilities and Resources

Simulation Tools

- Naval Simulation System (NSS)
- NETWARS/OPNET
- QualNet

Existing Communications Model Library

- COTS and GOTS protocols, devices, and systems
- OPNAV N61M C4ISR standard models

Scenario and Traffic Data models

- Navy Defense Reference Model (DRM)
  - Operational scenarios validated by Office of Naval Intelligence
- Probe and Information Exchange Requirement (IER) data
  - Import real probe traffic data into modeled networks

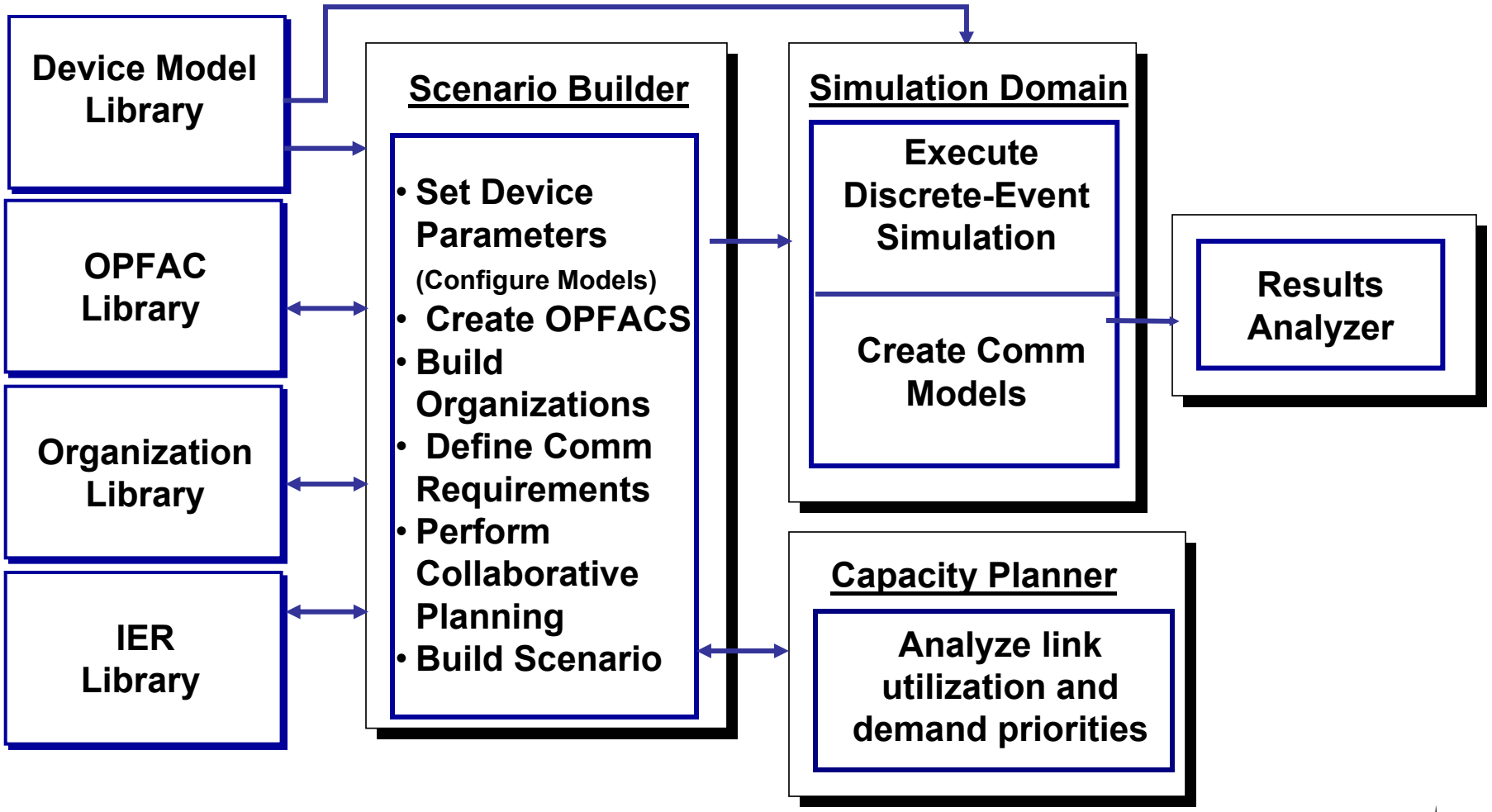
SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

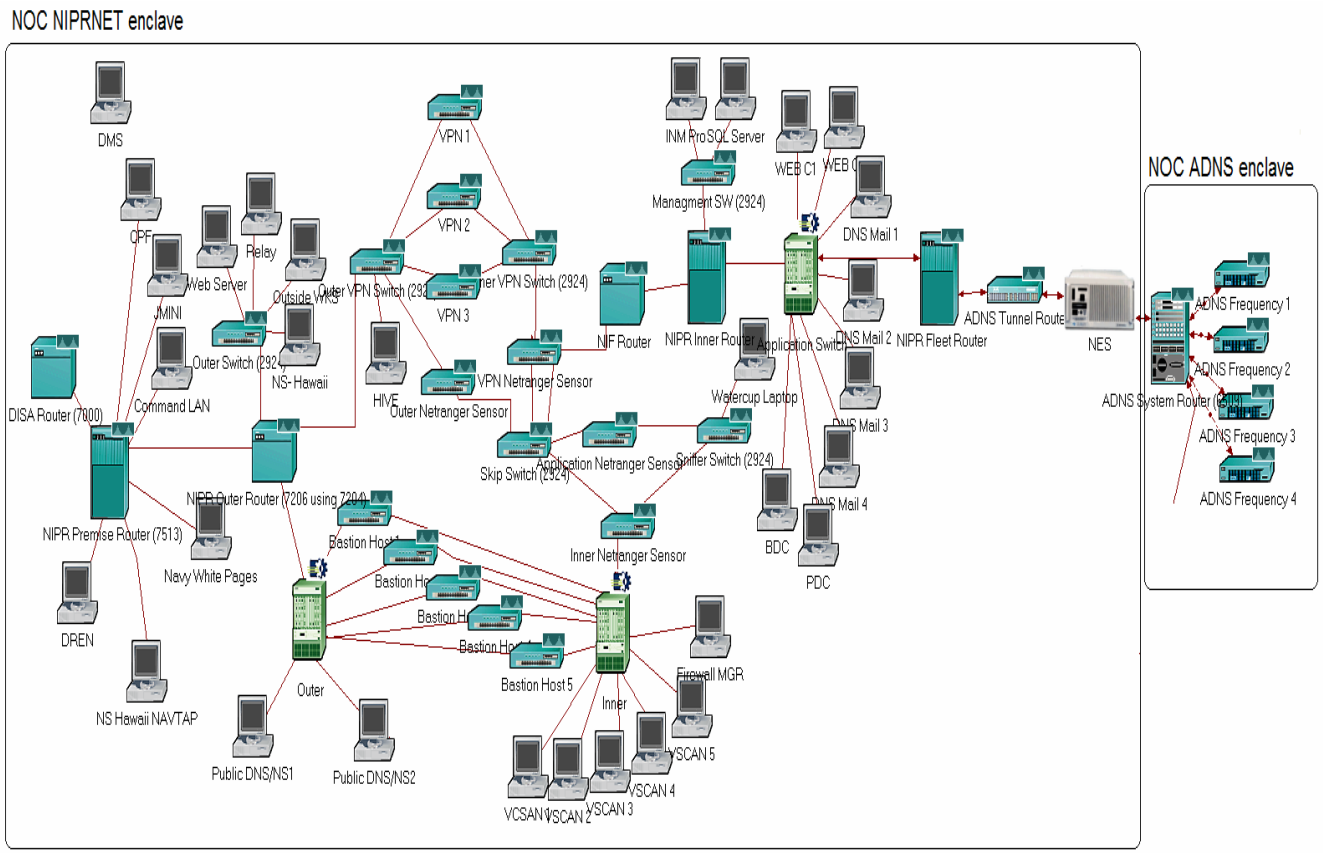
SPAWAR Systems Center San Diego

NETWARS Architecture



SPAWAR Systems Center San Diego

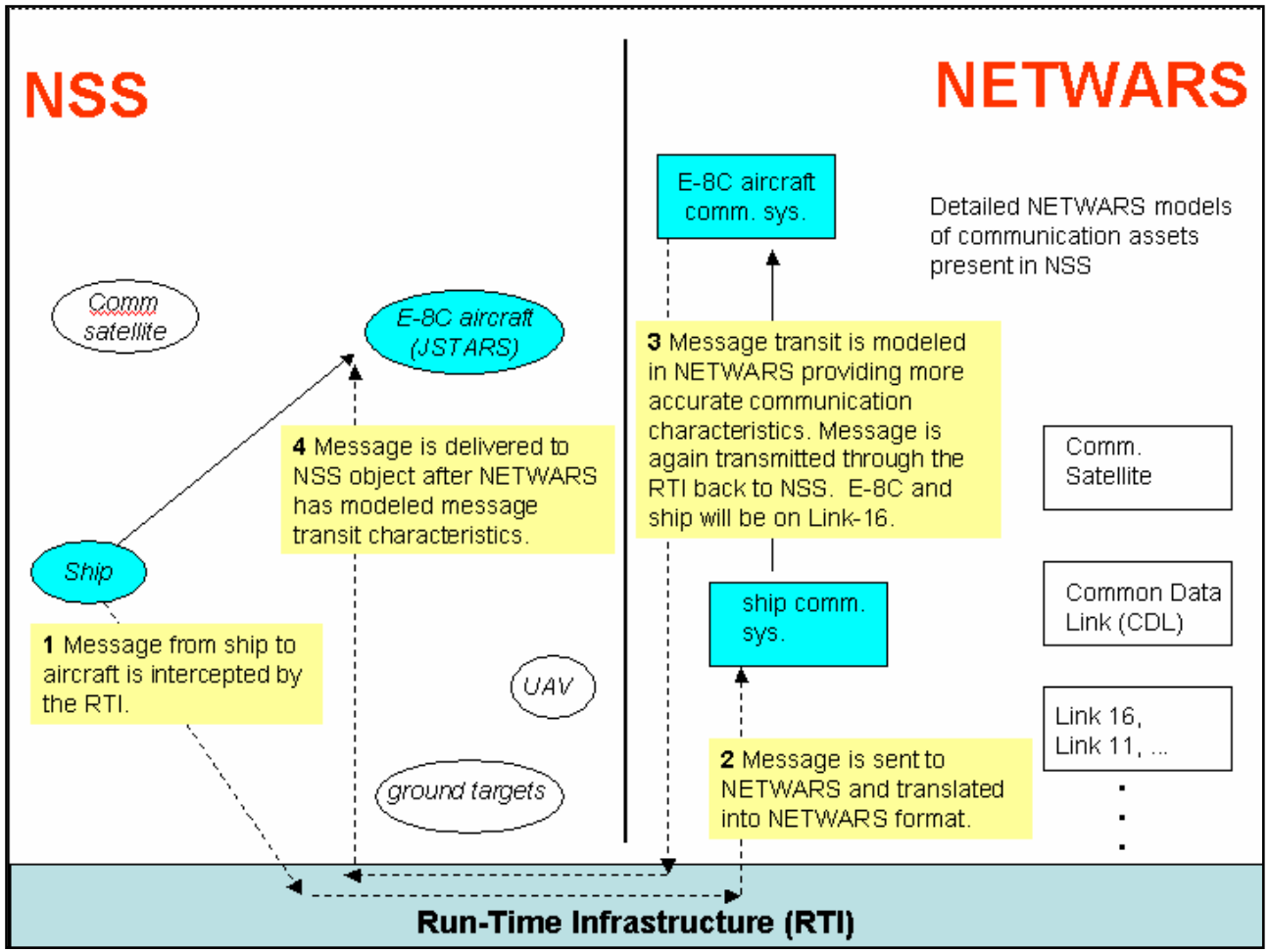
OPFACs of NIPRNET and ADNS Organizations



- 4 Network Operations Centers worldwide
- Templates: PRNOC SIPRNET & NIPRNET
- Template modification for UARNOC, IORNOC, ECRNOC

CCRP

NSS-NETWARS Integration Overview



SPAWAR
Systems Center
San Diego

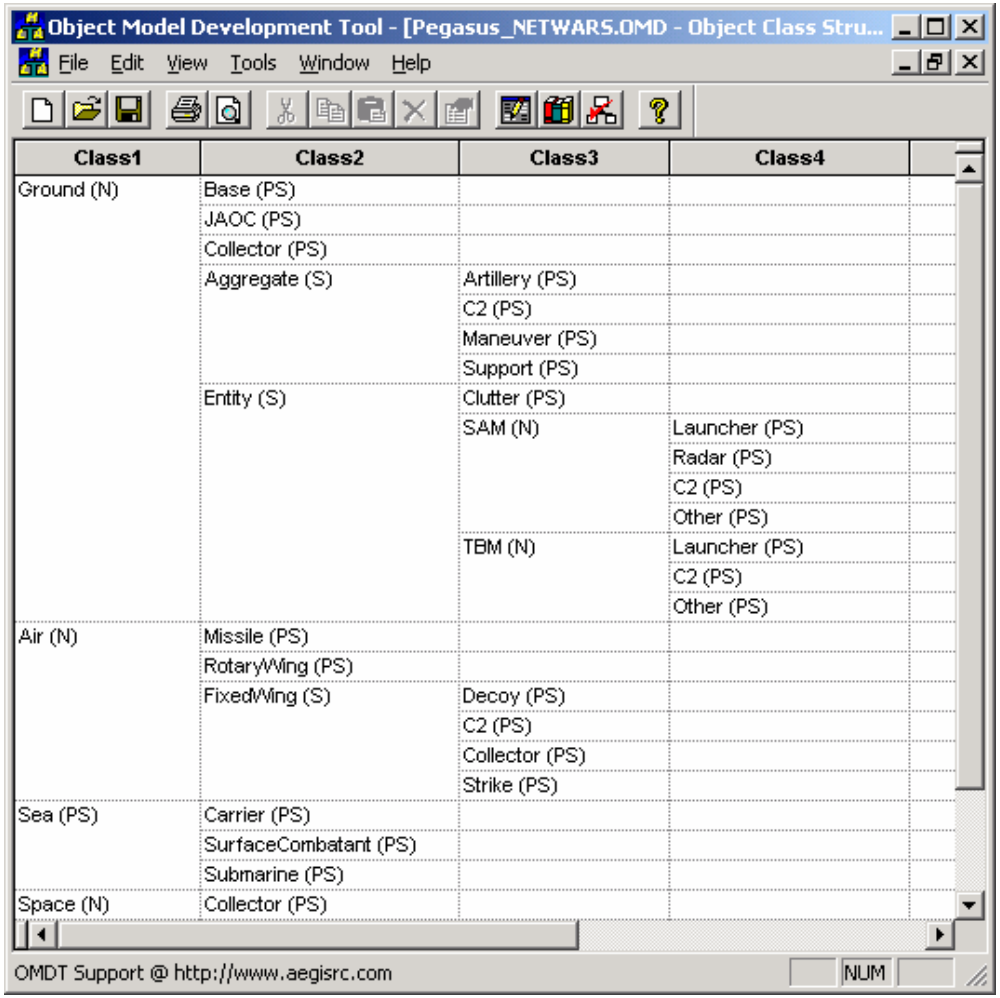
Overall Functionality

Two main features

- **Extension of the Pegasus Federation Object Model (FOM)**
  - *Combat_Transmission_Request* to notify NETWARS when to send a message
  - *Combat_transmission_Receipt* to return to NSS the status of the transmission, and delay if the transmission is successful
- **DRTI NETWARS Plug-in to enable NETWARS to interact with NSS. Three components**
  - DRTI Process Model and Model Modifications
  - DRTI NETWARS ESA Support Module
  - DRTI Management Module

SPAWAR Systems Center San Diego

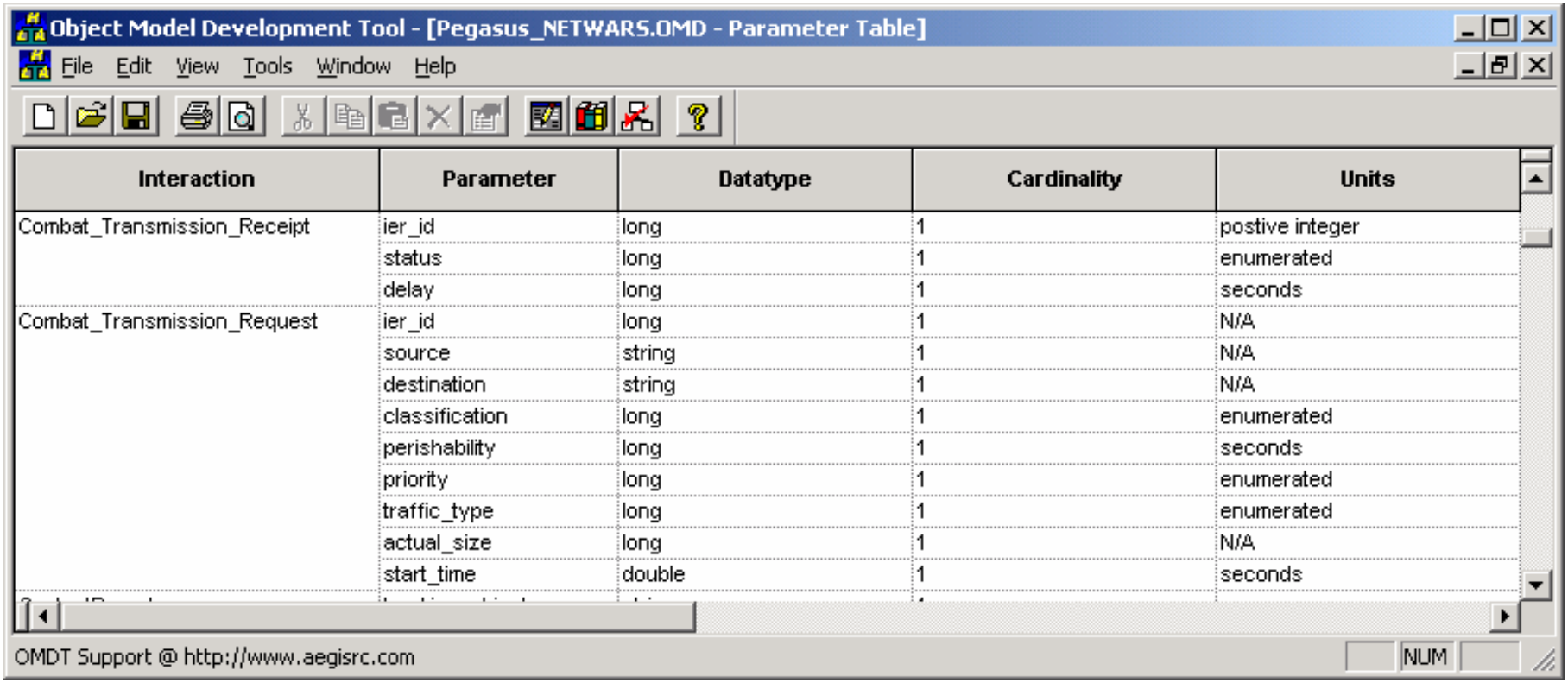
Federation Object Model Object Class Structure



Class1	Class2	Class3	Class4
Ground (N)	Base (PS)		
	JAOC (PS)		
	Collector (PS)		
	Aggregate (S)	Artillery (PS)	
		C2 (PS)	
		Maneuver (PS)	
		Support (PS)	
	Entity (S)	Clutter (PS)	
		SAM (N)	Launcher (PS)
			Radar (PS)
			C2 (PS)
			Other (PS)
		TBM (N)	Launcher (PS)
			C2 (PS)
			Other (PS)
Air (N)	Missile (PS)		
	RotaryWing (PS)		
	FixedWing (S)	Decoy (PS)	
		C2 (PS)	
		Collector (PS)	
		Strike (PS)	
Sea (PS)	Carrier (PS)		
	SurfaceCombatant (PS)		
	Submarine (PS)		
Space (N)	Collector (PS)		

SPAWAR
Systems Center
San Diego

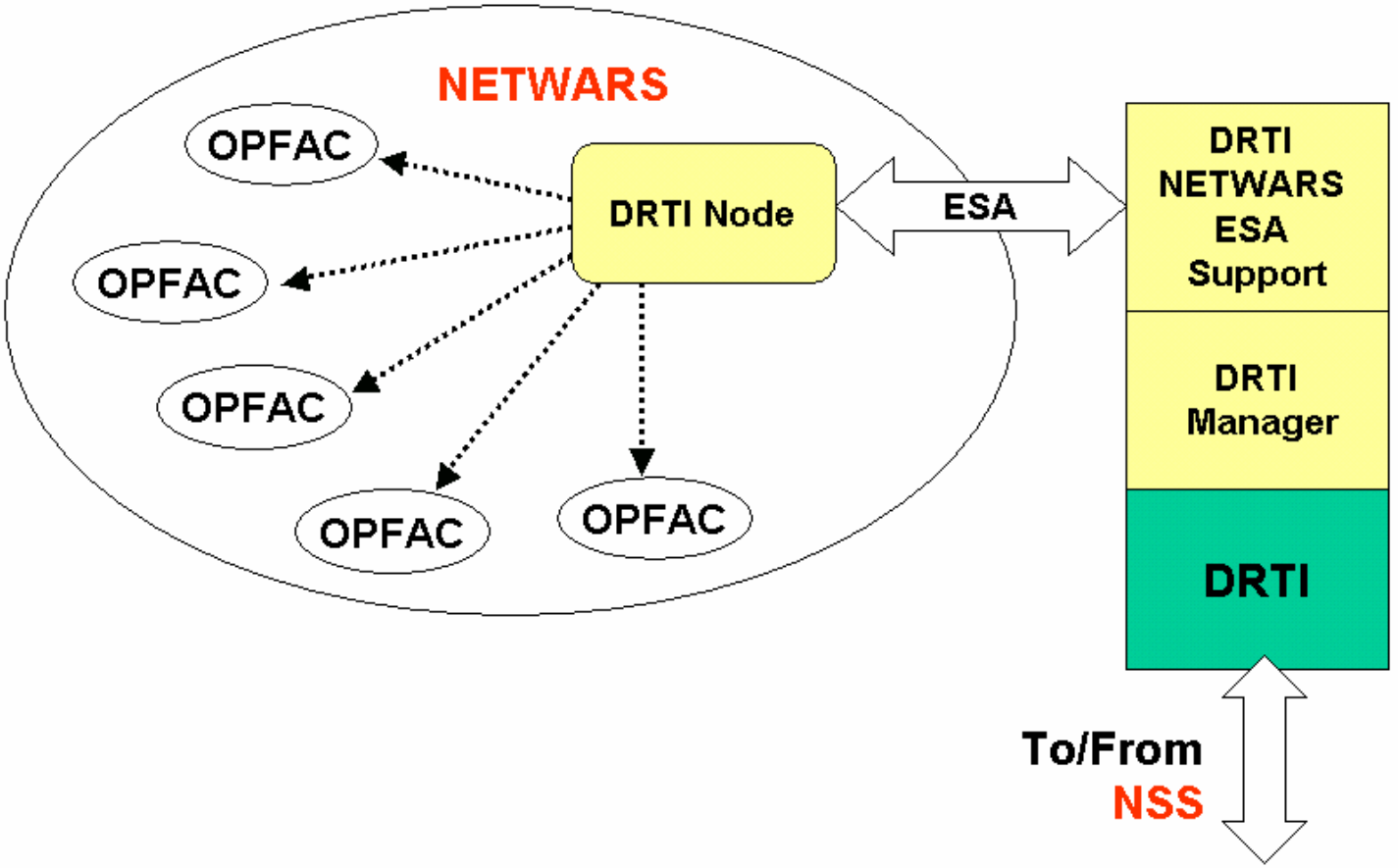
Federation Object Model Communications Interactions



Interaction	Parameter	Datatype	Cardinality	Units
Combat_Transmission_Receipt	ier_id	long	1	postive integer
	status	long	1	enumerated
	delay	long	1	seconds
Combat_Transmission_Request	ier_id	long	1	N/A
	source	string	1	N/A
	destination	string	1	N/A
	classification	long	1	enumerated
	perishability	long	1	seconds
	priority	long	1	enumerated
	traffic_type	long	1	enumerated
	actual_size	long	1	N/A
	start_time	double	1	seconds

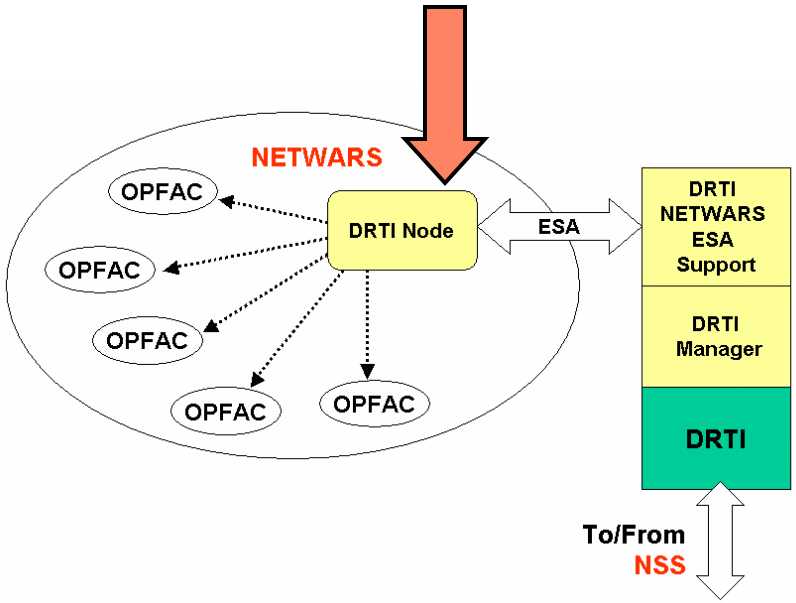
SPAWAR
Systems Center
San Diego

NSS-NETWARS Integration Architecture



SPAWAR
Systems Center
San Diego

DRTI Process Model and Model Modifications



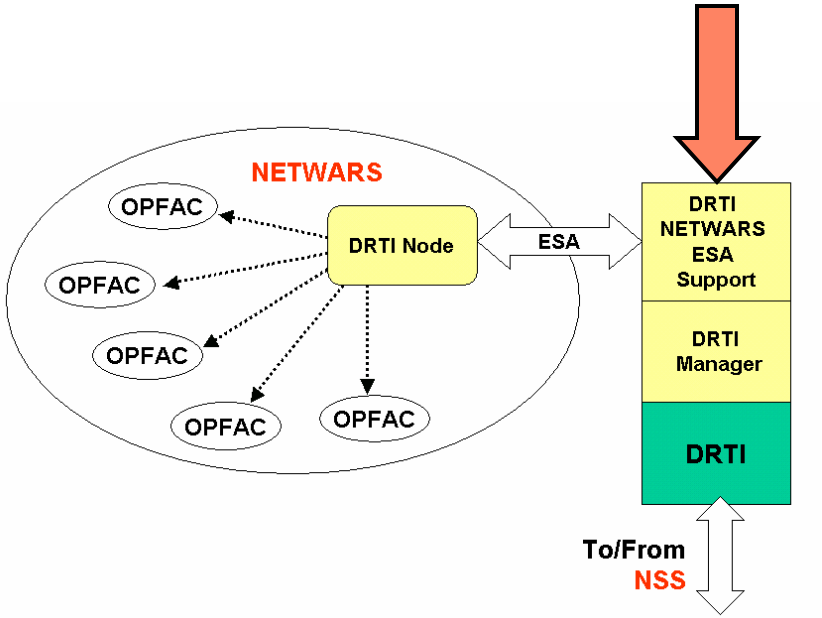
DRTI Process Model (of the DRTI Node Model) has two main tasks

- **Provide mechanism to apply position updates of entities in NSS to OPFACs in NETWARS**
- **Provide mechanism to initiate IERs and to return transmission status and delay back to NSS**

NETWARS process models *oe_iers* and *oe_status* are modified for sending a message from info provided by NSS, and to support capturing the delivery status of the message

SPAWAR Systems Center San Diego

DRTI NETWARS ESA Support Module

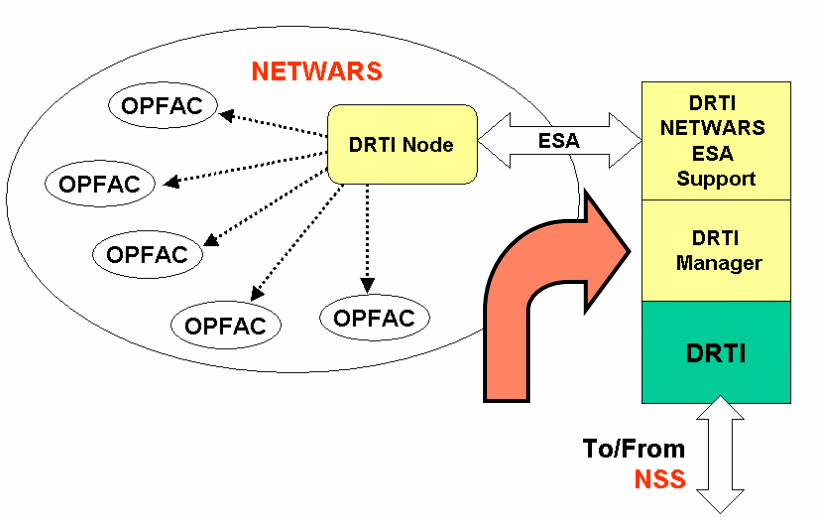


DRTI NETWARS ESA Module uses the OPNET's External Simulation Access (ESA) package to provide communication between NETWARS entities and DRTI.

- **ESA provides an interface to pass information into and out of the NETWARS domain for scheduling mobility events and sending messages.**
- **ESA provides services to control the execution of events in NETWARS/OPNET.**

SPAWAR
Systems Center
San Diego

DRTI Management Module



DRTI Management Module performs the following tasks

- Initialize DRTI.
- Subscribe all relevant objects published by NSS.
- Subscribe to the Combat_Transmission_Request interaction and publish the Combat_Transmission_Receipt.
- Provide services to DRTI NETWARS ESA Support Module to advance RTI time and deliver all messages held by DRTI.

SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

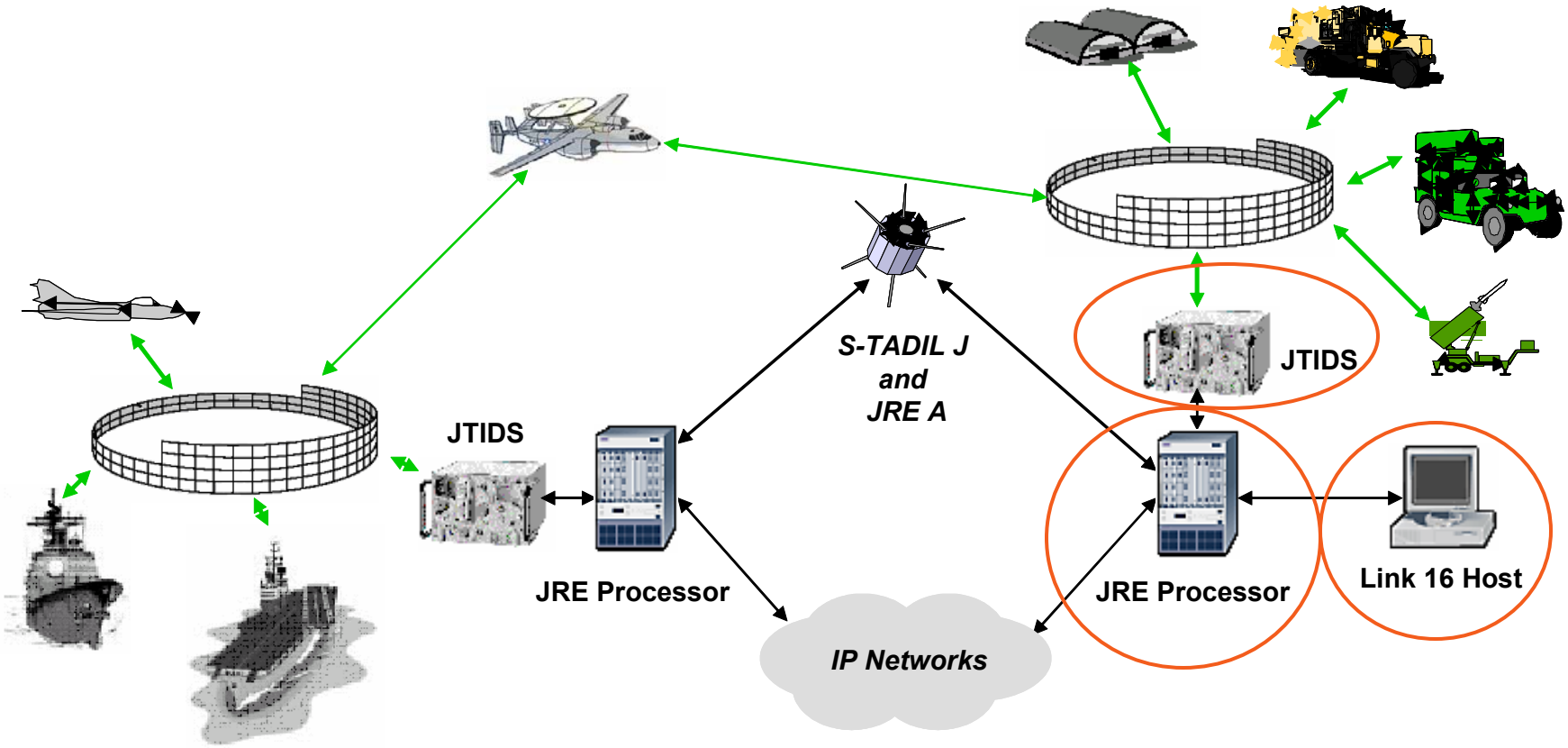
SPAWAR Systems Center San Diego

Link-16 Modeling and Simulation Efforts

- Link-16 model was originally developed using OPNET in September 2001 to support a Time Critical Strike (TCS) study sponsored by the Assistant Secretary of Navy for Research, Development, and Acquisition Chief Engineer (ASN RDA CHENG)
- Subsequently, the Link-16 model was reused in several simulation-based efforts at SSC San Diego. Throughout these studies, the model was enhanced to meet additional requirements and evolved into a fairly high-fidelity, general purpose Link-16 communications model
- In 2003, the Link-16 Program Management Office (via ONR) began to use the model for prototyping potential Link-16 system enhancements
- In February 2004, the NETWARS PMO decided to adopt the Navy Link-16 model as the standard for Link-16 modeling for all the Joint Services. SSC San Diego is currently supporting this NETWARS standardization effort, including user interface enhancements and additional Joint Range Extension (JRE) support

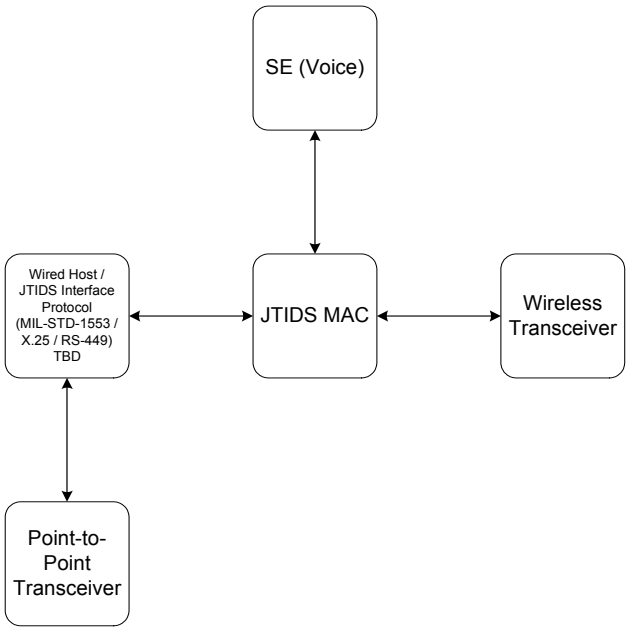
SPAWAR
Systems Center
San Diego

Link-16 Model Suite Devices



SPAWAR Systems Center San Diego

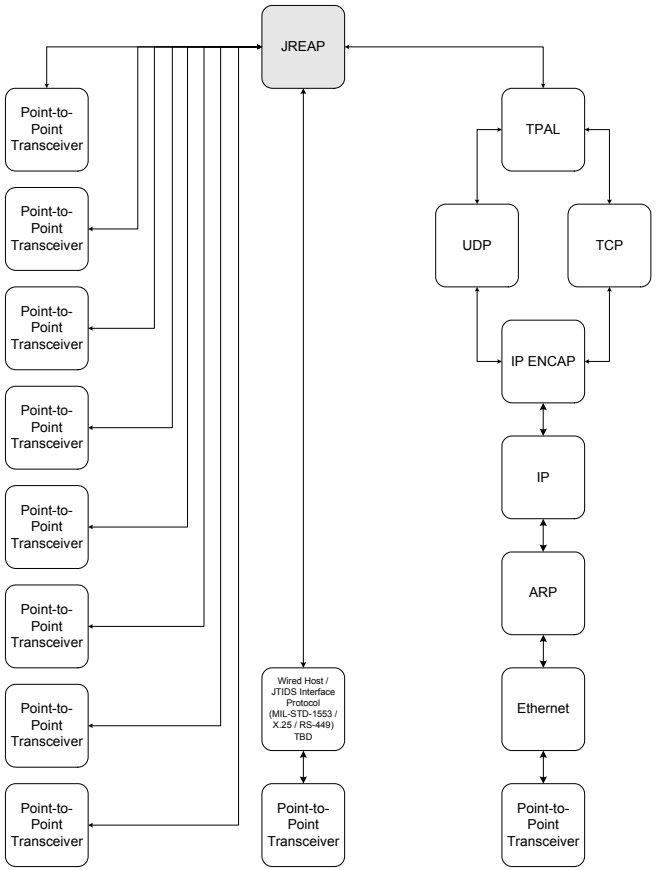
JTIDS Device Model



- **Three processors**
  - SE module for modeling voice IER generation and reception. (J-series messages are generated by tactical host and JRE Processor)
  - JTIDS MAC simulates the functionality of JTIDS terminal model
  - Wired Host/JTIDS Interface Protocol
- **Two interfaces**
  - Point-to-point wired transceiver
  - Wireless transceiver to communicate with other JTIDS device models

SPAWAR Systems Center San Diego

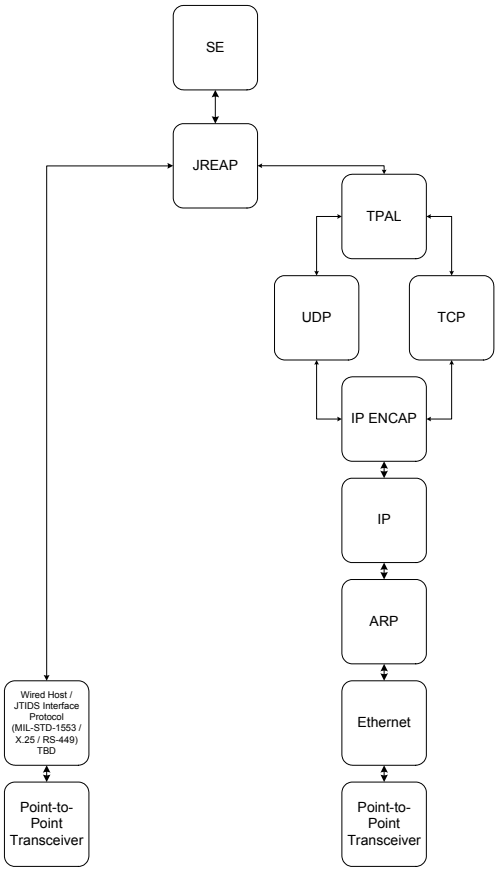
JRE Processor Device Model



- **JREAP, based on MIL-STD-3011, defines the protocols for transmission of Link-16 data over different type of long-haul media**
  - **JREAP-A: over broadcast SATCOM networks (e.g., MilStar and UHF DAMA)**
  - **JREAP-B: over point-to-point JRE media such as voice circuits – not supported by the JRE Processor Model**
  - **JREAP-C: over IP-based networks**
- **Ten interfaces**
  - **Four RS-232 ports**
  - **Four RS-422 ports**
  - **One 10/100BaseT ethernet port (JREAP-C)**
  - **One MIL-STD-1553B/X.25/RS-449 interface**

SPAWAR Systems Center San Diego

Link-16 Host Processor Device Model



- SE process model generates and receives J-series message traffic
- JREAP process model is an instance of the JREAP process model of the JRE Processor Device Model with modifications to support the local SE for generating and receiving J-series traffic
- Two interfaces
  - JREAP-C interface (10/100BaseT)
  - MIL-STD-1553B/X.25/RS-449 interface

SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

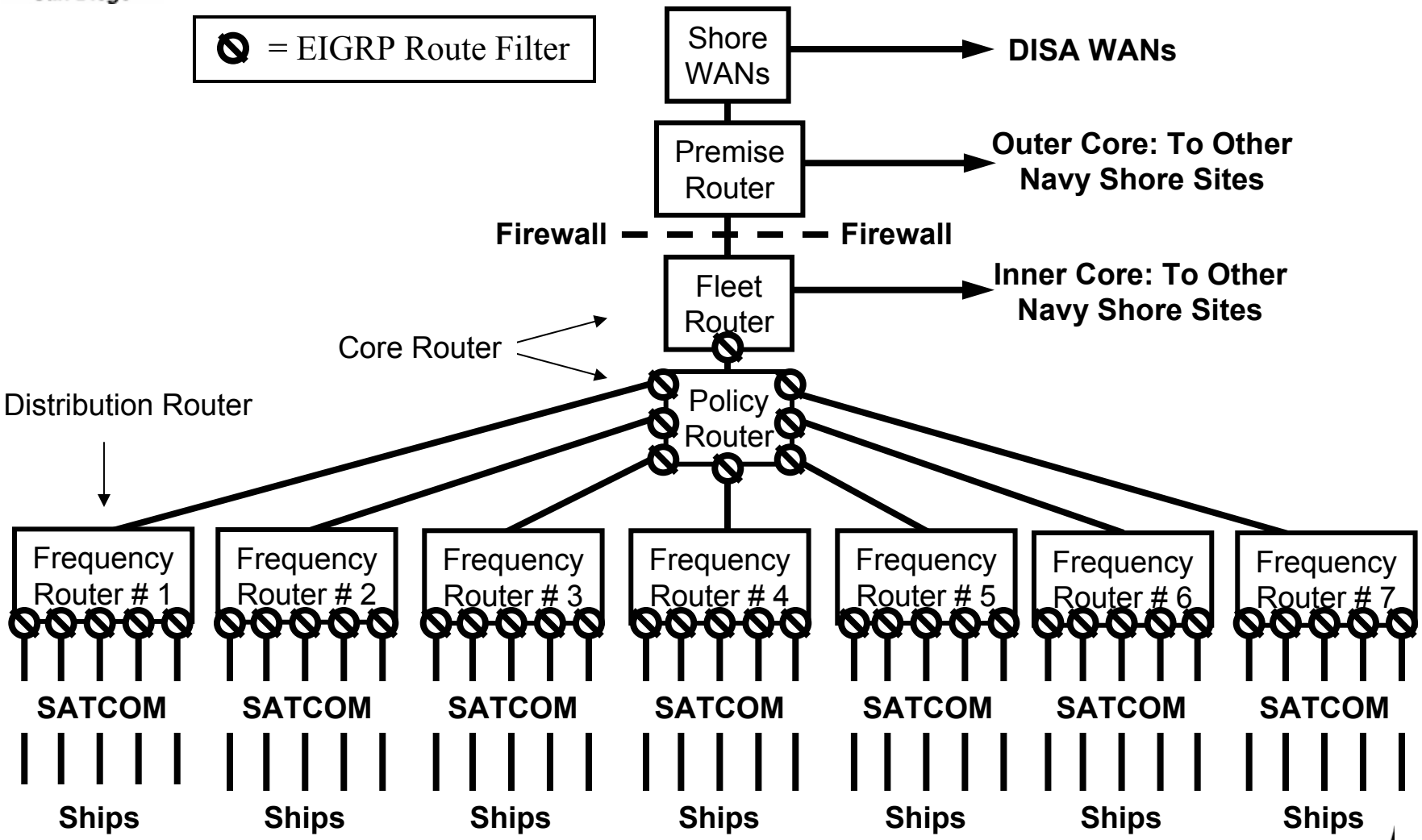
SPAWAR
Systems Center
San Diego

KSA FNC:
Toward a Unified Naval Network

- A Unified Naval Network will reduce network maintenance efforts and network outages between ships and shore sites
- Two routing architectures considered
  - The current Open Shortest Path First (OSPF) Design extended to a single worldwide routing domain
  - Proposed Traffic Flow Engineering (TFE) architecture using the Enhanced Interior Gateway Routing Protocol (EIGRP)
- A comparative study was conducted using the M&S tool QualNet

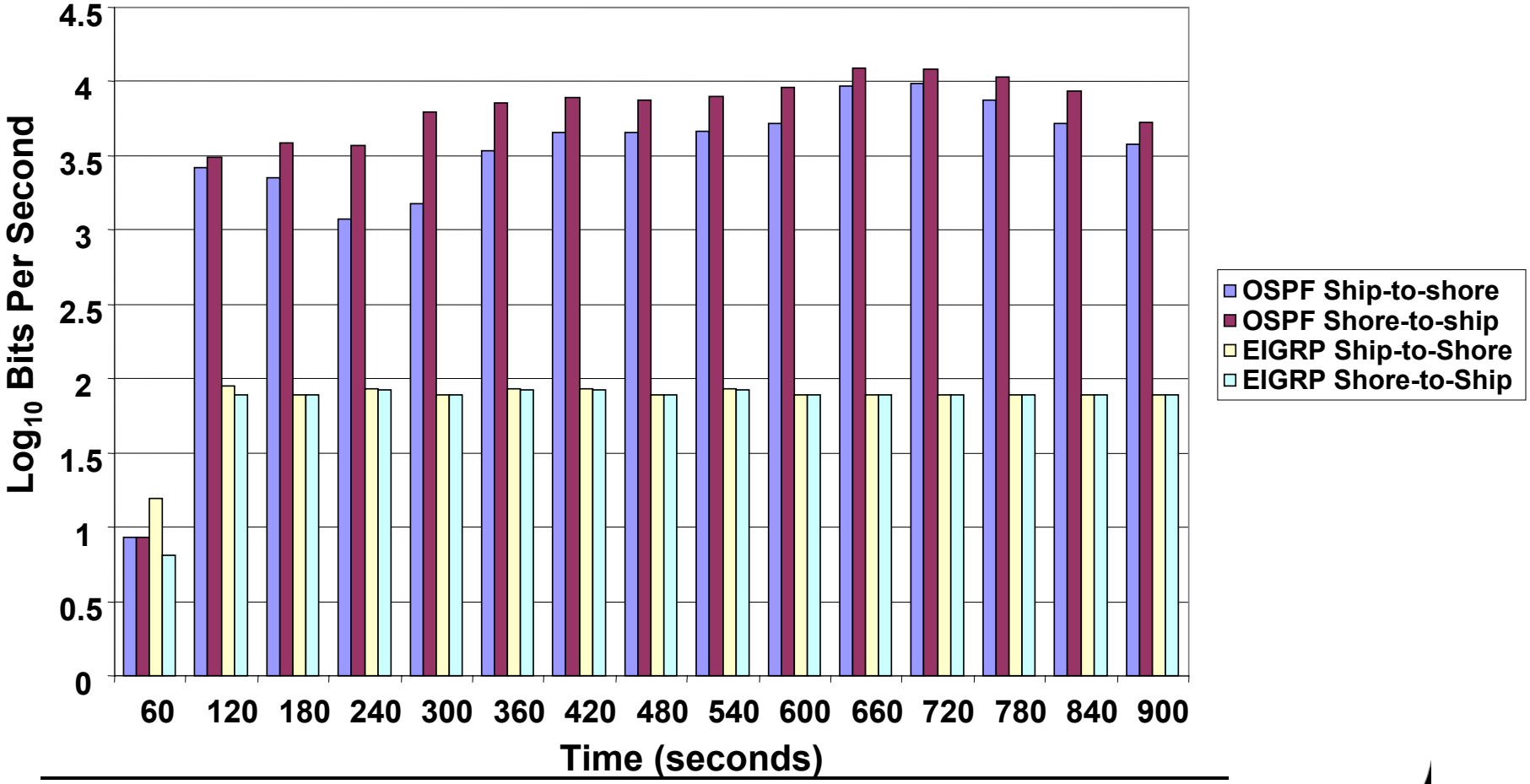
SPAWAR Systems Center San Diego

Route Filters within Navy Shore Site



SPAWAR Systems Center San Diego

OSPF vs EIGRP Bandwith Consumption on a SATCOM Link



CCRP

SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

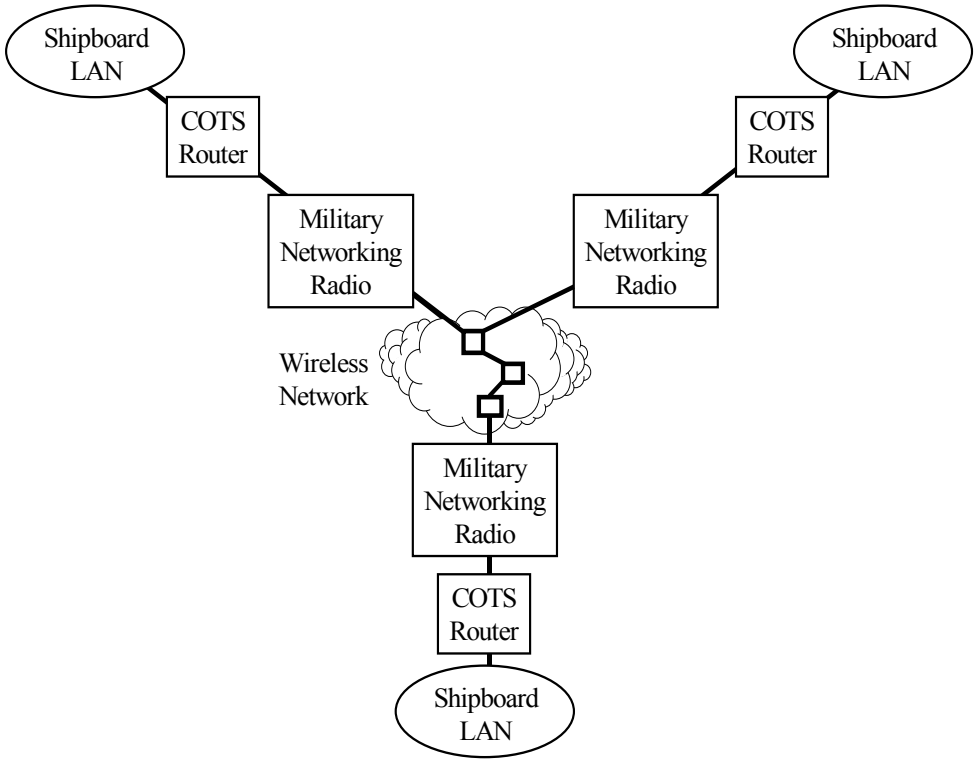
SPAWAR
Systems Center
San Diego

KSA FNC:
Simulation-Assisted Routing Protocol Design

- The Goals of the Intra Battle Group Wireless Networking (IBGWN) project of the ONR Naval Battle Force Network (part of KSA FNC) include better adaptive, mobile, wireless networks connecting multiple Naval platforms within a battle group as well as joint battle fields
- A Simulation-Assisted Routing Design Analysis, based on link-layer (Layer 2) routing, was conducted using the M&S tool QualNet.

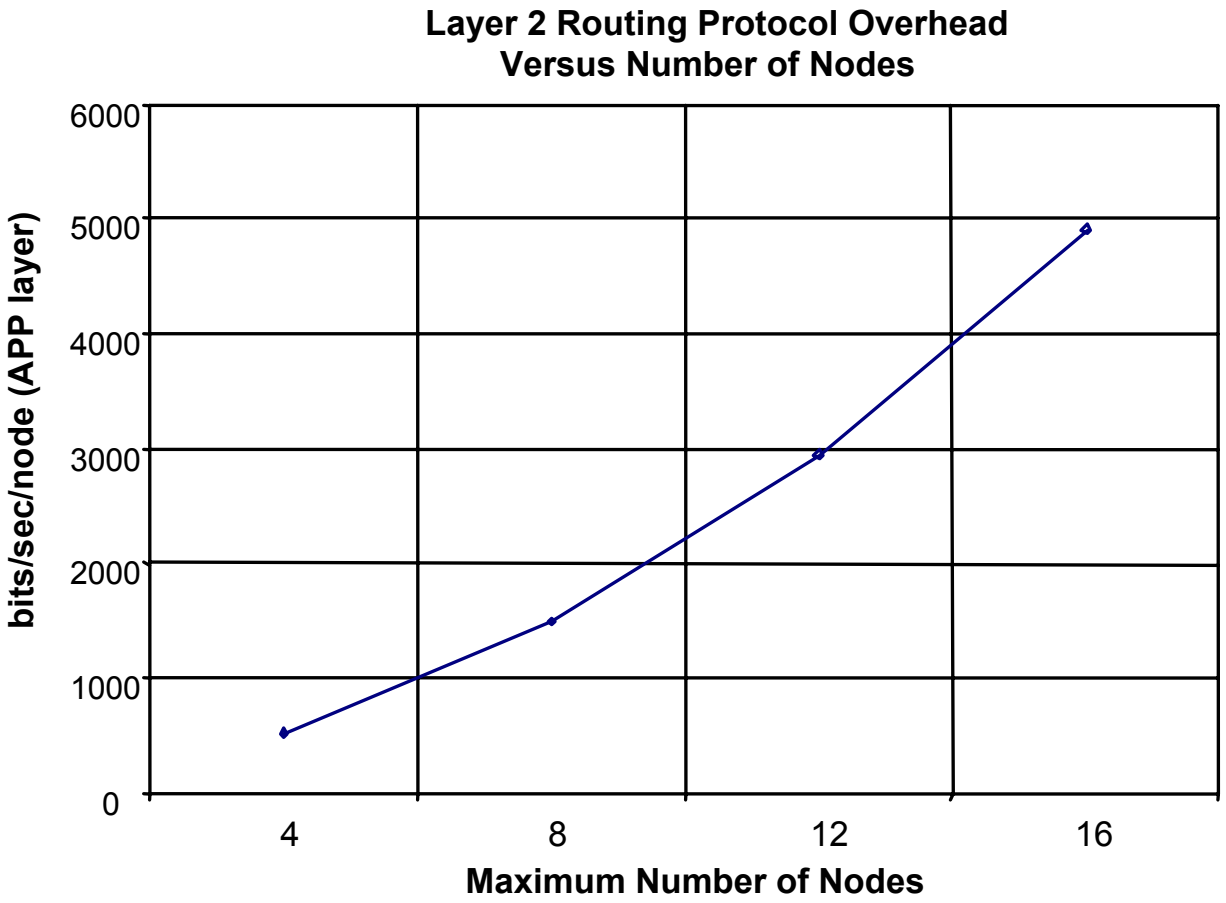
SPAWAR
Systems Center
San Diego

Routers and Networking Radios



SPAWAR
Systems Center
San Diego

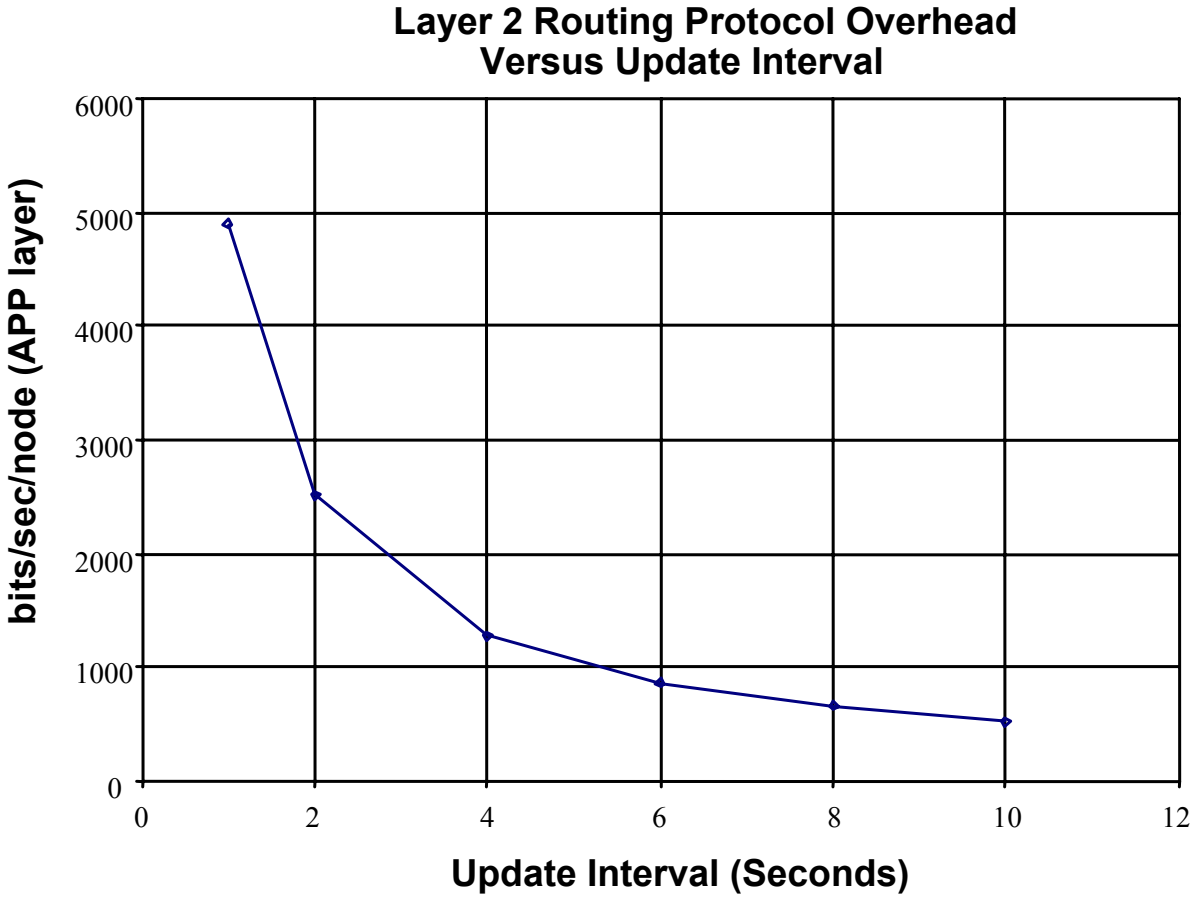
Routing Protocol Overhead vs. Number of Nodes



The connectivity matrix accounted for most of the bandwidth consumption

SPAWAR
Systems Center
San Diego

Routing Protocol Overhead vs. Update Interval



The increase in overhead is linear with the inverse of update interval

SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

SPAWAR
Systems Center
San Diego

Non-Intrusive Knowledge Suite (NIKS)

- Developed by the Cooperative Association for Internet Data Analysis (CAIDA, www.caida.org) under the direction of our Branch that served as the government Technical Agent for DARPA Network Modeling and Simulation (NMS) program
- Provide accurate and standardized datasets of network performance needed
  - to perform VV&A of M&S programs, and
  - to diagnose operational networks and systems
- Have applied for US Patent for NIKS.

SPAWAR Systems Center San Diego

Non-Intrusive Knowledge Suite (NIKS)

- NIKS operates on *tcpdump* (www.tcpdump.org) and CAIDA's *CoralReef* software.
- The main module of NIKS is *crl_delay* that records all relevant info (such as source and destination IP addresses and ports, sequence numbers, packet lengths) and derived statistics of latencies for each TCP connection
  - TCP Round Trip Times for all TCP packets at any ethernet port
  - One-way latency between two ethernet ports when both ports see the same packet
- Similar info for other observed protocols (such as UDP or ICMP) is also recorded.

SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

SPAWAR
Systems Center
San Diego

Lab and Field Experimentation

- Our lab and field experimentation efforts are associated with
  - FORCEnet (Navy's initiative)
  - Joint Rapid Architecture Experimentation (JRAE) (Joint Service initiative)
- These experimentation efforts complement our M&S activities, providing for VV&A and enabling studies with greater focus on operational environment factors and Human Systems Integration (HIS)

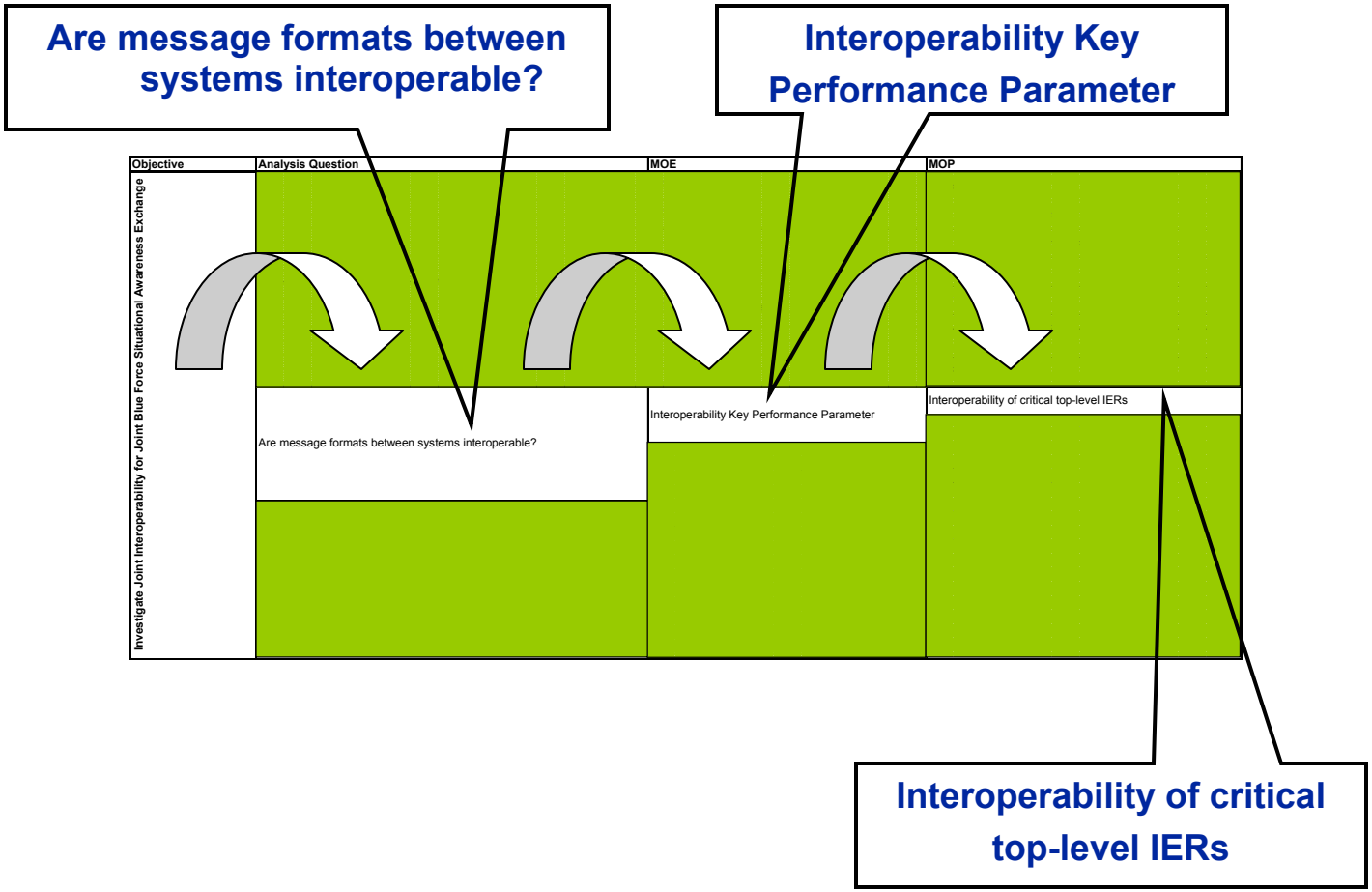
SPAWAR
Systems Center
San Diego

Lab and Field Experimentation: Process

- **Metrics**
  - Clear experimentation objectives facilitate the formation of analysis questions
- **Replication of Network and Applications**
  - Experimentation objectives determine required and acceptable fidelity levels
- **Data Collection**
  - Metrics derived from objectives dictate what data collection is required
- **Experiment Execution**
  - Monitoring collection devices (for data quality) and administering questionnaires/interviews with system operators (for HIS Metrics)
- **Analysis**
  - Quick-Look Report and Final Report

SPAWAR Systems Center San Diego

Data Collection Taxonomy of Objectives, Analysis Questions, MOEs, and MOPs



SPAWAR
Systems Center
San Diego

Outline

- Introduction
- Navy Network Warfare Simulation (NETWARS)
- Link-16 Modeling and Simulation (M&S) Efforts
- Efforts in Support of Knowledge Superiority and Assurance (KSA) Future Naval Capacity (FNC)
  - Toward a Unified Naval Network
  - Simulation-Assisted Protocol Design
- Related Efforts
  - Non-Intrusive Knowledge Suite (NIKS)
  - Lab and Field Experimentation
- Conclusion

SPAWAR
Systems Center
San Diego

Conclusion

Making Use of the Full Spectrum of Modeling and Simulation (M&S) environments is the key focus of our activities in Support of Network Warfare Analysis

- Develop standard, reusable, interoperable models to reduce cost and enhance model assessment time
- Work with all facets of the M&S community, which includes Joint Services, government agencies, deployed operational commands, academia and industry, to support the warfighter with the best possible analytical capability
- Continue to enhance our capability by working with
  - DoD High Performance Computing Modernization Office (HPCMO) to improve simulation runtime performance,
  - DARPA Network Modeling and Simulation (NMS) program office to leverage new technologies in M&S,
  - DMSO and NAVMSMO to support policy, standards and guidance.

SPAWAR
Systems Center
San Diego

Q&A